One-VA Technical Reference Model

Version 10.6

Version History

Date	Version	Description	Author
May-25-10	10.6	Document generated from TRM Website	TRM Team

Table of Contents

Purpose ... 26
1) Approved Health Segment Technologies/Standards List ... 27
2) Approved Health Segment Technologies/Standards Entries ... 39
2.1) 7 kHz Audio-Coding within 64 kbit/s ... 39
2.2) A Framework for IP Based Virtual Private Networks (VPNs) ... 41
2.3) Access Control ... 43
2.4) Access Control Framework ... 45
2.5) Active Data Guard ... 47
2.6) Active Directory ... 49
2.7) Advanced Billing Concept (ABC) ... 52
2.8) Advanced Encryption Standard (AES) ... 54
2.9) Advanced Video Coding for Generic Audiovisual Services ... 56
2.10) AIX ... 58
2.11) ANT ... 62
2.12) Apache Cactus ... 65
2.13) Apache Commons ... 69
2.14) Apache HTTP Server ... 73
2.15) Apache POI ... 77
2.16) Apache Struts ... 80
2.17) Apache Tomcat ... 86
2.18) Application Oriented Sites ... 89
2.19) Architecture for IP Address Allocation with CIDR ... 90
2.20) Audit Services ... 92
2.21) Basic Transition Mechanisms for IPv6 Hosts Routers ... 94
2.22) Bing Maps ... 96
2.23) Biometric Application Programming Interface (BioAPI) ... 99
2.24) Biometric Information Management and Security ... 102
2.25) Biometric Services ... 104
2.26) BIRT ... 106
2.27) BlazeDS ... 110
2.28) BMC Mainview ... 113
2.29) BMC Performance Manager ... 115

2.30) Bobby 119
2.31) Border Gateway Protocol (BGP) 122
2.32) Broadband Audiovisual Communication Systems and Terminals 124
2.33) BusinessWare 127
2.34) Cache Database Engine 130
2.35) Cache JDBC Driver 135
2.36) Call Signalling Protocols and Media Stream Packetization 137
2.37) Carrier Sense Multiple Access with Collision Detection (CSMA/CD) 139
2.38) Cascading Style Sheets (CSS) 142
2.39) Cascading Style Sheets Mobile Profile (CSS-Mobile) 144
2.40) Castor XML 146
2.41) Checksum Hash Value 148
2.42) Classless Inter-Domain Routing (CIDR) 150
2.43) Coding of Speech Using Low-Delay Code Excited Linear Prediction 152
2.44) Common Biometric Exchange Formats Framework (CBEFF) 154
2.45) Common Language Infrastructure (CLI) 156
2.46) Common Object Request Broker Architecture (CORBA) 158
2.47) Common Warehouse Metamodel (CWM) 161
2.48) Computer Based Training Exchange 163
2.49) Computer Graphics Metafile (CGM) 165
2.50) Confidentiality Framework 167
2.51) Confidentiality Services 169
2.52) Configuration Management 171
2.53) Control Protocol for Multimedia Communication 173
2.54) Cryptographic Algorithm Implementation Requirements for ESP and AH 175
2.55) Current Dental Terminology (CDT) 177
2.56) Current Procedural Terminology (CPT) 180
2.57) Data Center 182
2.58) Data Encryption Standard (DES) 184
2.59) Data Format Classification 186
2.60) Data Format for Fingerprint, Facial, & SMT Information 188
2.61) Data Integrity 190
2.62) Data Oriented Sites 192
2.63) Data Protocols for Multimedia Conferencing 194

2.64) Data Protocols for Multimedia Conferencing - Generic Conference Control 196
2.65) Database Services 198
2.66) Datatypes for DTDs (DT4DTD) 200
2.67) Datejs 202
2.68) Diagnosis-Related Group (DRG) 204
2.69) Diagnostic and Statistical Manual of Mental Disorders (DSM) 207
2.70) Differentiated Services (DS) Field in IPv4 and IPv6 Headers 209
2.71) Digital Compression and Coding of Continuous-Tone Still Images 211
2.72) Digital Imaging and Communications in Medicine (DICOM) 214
2.73) Digital Signature 216
2.74) Digital Signature Standard (DSS) 217
2.75) Directory Server 219
2.76) Discovery Services 222
2.77) Diskeeper 223
2.78) Domain Name Service 225
2.79) Domain Name System (DNS) Configuration Options 227
2.80) Domain Name System (DNS) Extensions 229
2.81) Domain Name System (DNS) Structure and Delegation 231
2.82) Dynamic Host Configuration Protocol (DHCP) 233
2.83) Dynamic Host Configuration Protocol Configuration of IPsec Tunnel Mode (DHCPv4) 236
2.84) Dynamic Host Configuration Protocol for IPv6 (DHCPv6) 238
2.85) Dynamic Server Side Display 240
2.86) Dynamic Updates in the Domain Name System (DNS UPDATE) 242
2.87) ebXML Collaboration Protocol Profile and Agreement (ebXML CPPA) 244
2.88) ebXML Messaging Service (ebMS) 246
2.89) ebXML Registry Information Model (ebRIM) 249
2.90) ebXML Registry Services (ebRS) 251
2.91) Eclipse 254
2.92) Eclipse Modeling Framework (EMF) 257
2.93) eGate Integrator 260
2.94) Electronic Authentication of Health Care Information 263
2.95) Encryption Algorithm and IPsec 265
2.96) Encryption Services 267
2.97) Enhanced Security Services for S/MIME 269

2.98) Environmental Protection Agency - Substance Registry System (EPA-SRS) 271
2.99) ERwin Data Modeler 273
2.100) Escrowed Encryption Standard 275
2.101) Establishing Communication Between Multiple Audiovisual Terminals 278
2.102) European Article Number (EAN-13) 280
2.103) Exchange Server 282
2.104) Extended Simple Mail Transfer Protocol (ESMTP) 284
2.105) eXtensible Access Control Markup Language (XACML) 286
2.106) Extensible Authentication Protocol (EAP) 288
2.107) Extensible Authentication Protocol Tunneled Transport Layer Security (EAP-TTLS) 291
2.108) Extensible HyperText Markup Language (XHTML) 293
2.109) Extensible Markup Language (XML) 295
2.110) Fault Management 299
2.111) FDR 300
2.112) Fiber Distributed Data Interface (FDDI) 302
2.113) File Transfer Protocol (FTP) 305
2.114) File Transfer Protocol (FTP) Extensions 308
2.115) File Transfer Protocol Services 310
2.116) Fire Walling 311
2.117) Firefox 313
2.118) Flex SDK 316
2.119) Frame Structure in Audiovisual Teleservices 319
2.120) Frame-synchronous Control and Indication Signals for Audiovisual Systems 321
2.121) General Parallel File System (GPFS) 324
2.122) Google Maps 326
2.123) Graphics Interchange Format (GIF) 329
2.124) Health Information Data Exchange 331
2.125) Healthcare Common Procedure Coding System (HCPCS) 332
2.126) Hibernate Core 334
2.127) HL7 338
2.128) HP-UX 342
2.129) Human Gene Nomenclature (HGN) 346
2.130) HyperText Markup Language (HTML) 348
2.131) Hypertext Transfer Protocol (HTTP) 350

2.132) Hypertext Transfer Protocol Services 352
2.133) Identification Authentication 354
2.134) Identification Cards - Integrated Circuit(s) Cards With Contacts 356
2.135) ImageGear 358
2.136) Information Access Privileges to Health Information 361
2.137) InfoSphere Data Architect 363
2.138) InstallShield 367
2.139) International Classification of Diseases (ICD) 370
2.140) International Nonproprietary Names (INN) 372
2.141) Internet Control Message Protocol (ICMP) 374
2.142) Internet Explorer 376
2.143) Internet Information Services (IIS) 380
2.144) Internet Key Exchange (IKE) 382
2.145) Internet Message Access Protocol (IMAP) 385
2.146) Internet Message Format 387
2.147) Internet Protocol (IP) 389
2.148) Internet Protocol Version 6 (IPv6) 391
2.149) Internet Web 393
2.150) Intranet Web 395
2.151) Intrusion Detection and Prevention Systems (IDPS) 396
2.152) Intrusion Detection Devices 398
2.153) IP Authentication Header (AH) 400
2.154) IP Encapsulating Security Payload (ESP) 402
2.155) IP Network Address Translator (NAT) 404
2.156) IP Routing Services 407
2.157) IPsec Transport Mode for Dynamic Routing 408
2.158) IPsec-Network Address Translation (NAT) 411
2.159) IPv6 Client Services 413
2.160) IPv6 over Point-to-Point Protocol (PPP) 414
2.161) IPv6 Performance 416
2.162) IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCPv6) 418
2.163) IPv6/IPv4 Dual Stack Internet Access Service Model 420
2.164) iText Core 422
2.165) Java AVK 426

2.166) Java Data Objects (JDO) 430
2.167) Java EE 432
2.168) Java SE 438
2.169) JavaScript 443
2.170) JAWS 447
2.171) JAXB Reference Implementation 450
2.172) JAXP Reference Implementation 454
2.173) JPEG 457
2.174) JPEG 2000 460
2.175) JProbe 463
2.176) JRules Business Rules Management Server 466
2.177) JRules Rule Execution Server 470
2.178) JRules Rule Studio 473
2.179) JRules Scenario Manager 475
2.180) JRules Team Server 478
2.181) JUnit 480
2.182) Key Management Using ANSI X9.17 484
2.183) Keyed-Hash Message Authentication Code (HMAC) 486
2.184) Layer Two Tunneling Protocol (L2TP) 488
2.185) Lightweight Directory Access Protocol (LDAP) 490
2.186) Lightweight EAP (LEAP) 494
2.187) Local Area Network (LAN) 496
2.188) Log4J 499
2.189) Logical Observation Identifiers Names and Codes (LOINC) 502
2.190) Mail Services 504
2.191) Malicious Code Detection 505
2.192) Management Information Base (MIB) 507
2.193) Media Servers 510
2.194) Medical Device Communications 511
2.195) Medical Device Interoperability 514
2.196) Medical Radiology Images Exchange 515
2.197) Mercury LoadRunner 516
2.198) Mercury WinRunner 519
2.199) Messaging Workbench (MWB) 523

2.200) Metropolitan Area Network Services 526
2.201) Mirth Connect 528
2.202) MPEG-1 530
2.203) MPEG-2 533
2.204) MPEG-4 536
2.205) Multimedia Transport 540
2.206) Multiplexing Protocol for Low Bit Rate Multimedia Communication 542
2.207) Multipoint Binary File Transfer Protocol 544
2.208) Multipoint Communication Service (MCS) - Service Definition 546
2.209) Multipoint Communication Service (MCS) Protocol 549
2.210) Multipoint Control Units for Audiovisual Systems 551
2.211) Multipoint Still Image and Annotation Protocol 553
2.212) Multiprotocol Label Switching (MPLS) Architecture 555
2.213) Multipurpose Internet Mail Extensions (MIME) 557
2.214) MyEclipse 560
2.215) Narrow-band Visual Telephone Systems and Terminal Equipment 564
2.216) National Cancer Institute Thesaurus (NCIt) 566
2.217) National Drug Code (NDC) 568
2.218) National Drug File – Reference Terminology (NDF-RT) 570
2.219) Native Audio Formats 572
2.220) Native Document Formats 573
2.221) Native Graphics Formats 575
2.222) Native Video Formats 576
2.223) NCPDP Telecommunication Standards 577
2.224) Neighbor Discovery for IPv6 579
2.225) NetBackup 582
2.226) Network Address Translation - Protocol Translation (NAT-PT) 584
2.227) Network Transport 586
2.228) Network-specific Data Protocol Stacks for Multimedia Conferencing 588
2.229) Object Linking and Embedding, Database (OLE DB) 590
2.230) Objects and Attributes for Access Control 592
2.231) Office Open XML 594
2.232) Open Database Connectivity (ODBC) 596
2.233) Open Graphics Library (OpenGL) 599

2.234) Open Shortest Path First (OSPF) Protocol 601
2.235) OpenVMS 603
2.236) Oracle Database 605
2.237) Oracle JDBC Drivers 609
2.238) Packet-Based Multimedia Communications Systems 612
2.239) Parallel Sysplex 614
2.240) Password Services 616
2.241) Performance Management 618
2.242) Person Identification Service (PIDS) 620
2.243) Pharmacological Orders Exchange 622
2.244) PlateSpin Migrate 623
2.245) PlateSpin PowerConvert 625
2.246) PlateSpin Protect 627
2.247) Point-of-care Medical Device Communication 630
2.248) Point-to-Point Protocol (PPP) 632
2.249) Portable Document Format (PDF) 635
2.250) Portable Network Graphics (PNG) 637
2.251) Portlet 639
2.252) Post Office Protocol (POP) 641
2.253) PPP Triple-DES Encryption Protocol (3DESE) 643
2.254) Primavera TeamPlay 646
2.255) Processor Area Network (PAN) Manager 648
2.256) Protected Extensible Authentication Protocol (PEAP) 650
2.257) Public Key Infrastructure 652
2.258) Pulse Code Modulation (PCM) of Voice Frequencies 655
2.259) Radio Frequency Management 657
2.260) Rational Asset Manager 659
2.261) Rational Build Forge 662
2.262) Rational ClearCase with MultiSite 666
2.263) Rational ClearQuest with MultiSite 669
2.264) Rational Functional Tester 673
2.265) Rational Manual Tester 676
2.266) Rational Performance Tester 680
2.267) Rational PurifyPlus 683

2.268) Rational Quality Manager 685
2.269) Rational Requirements Composer 689
2.270) Rational RequisitePro 692
2.271) Rational Robot 696
2.272) Rational Rose 698
2.273) Rational RUP 700
2.274) Rational Software Architect 702
2.275) Rational Software Modeler 706
2.276) Rational Team Concert 710
2.277) Rational TestFactory 714
2.278) Rational TestManager 716
2.279) Red Hat Linux 719
2.280) Reflections 723
2.281) Regulations and Procedures for Federal Radio Frequency Management 726
2.282) Remote Access Protocol 728
2.283) Remote Authentication Dial In User Service (RADIUS) 730
2.284) Resource-Based Relative Value Scale (RBRVS) 732
2.285) Rich Text Format (RTF) 734
2.286) RoboHelp 736
2.287) RxNorm 740
2.288) Scalable Vector Graphics (SVG) 742
2.289) Secure Code Design 744
2.290) Secure Hash Standard (SHS) 745
2.291) Secure Hypertext Transfer Protocol (S-HTTP) 747
2.292) Secure Remote Access with L2TP 749
2.293) Secure/Multipurpose Internet Mail Extensions (S/MIME) Certificate Handling 751
2.294) Secure/Multipurpose Internet Mail Extensions (S/MIME) Message Spec 754
2.295) Securing Layer Two Tunneling Protocol (L2TP) with IPsec 756
2.296) Security Architecture for the Internet Protocol (IP) 758
2.297) Security Architecture for the Internet Protocol (IPSec) 760
2.298) Security Assertion Markup Language (SAML) 762
2.299) Security Requirements for Cryptographic Modules 765
2.300) Security Token 767
2.301) Servers 769

2.302) SharePoint Server 771
2.303) Simple Mail Transfer Protocol (SMTP) 773
2.304) Simple Network Management Protocol (SNMP) 776
2.305) Simple Object Access Protocol (SOAP) 778
2.306) Single Sign On 781
2.307) SiteMinder Web Access Manager 783
2.308) Solaris 786
2.309) Spring Framework 789
2.310) Spry Framework 795
2.311) SQL Server 798
2.312) Stateless Dynamic Host Configuration Protocol (DHCPv6) 802
2.313) Static Display 805
2.314) Storage 806
2.315) Strobe 808
2.316) Structured Query Language (SQL) 811
2.317) Synchronous Optical Network (SONET) 815
2.318) System for Establishing Communication Between Audiovisual Terminals 818
2.319) Systematized Nomenclature of Medicine-Clinical Terms (SNOMED CT) 820
2.320) TeamPage 823
2.321) TELNET 826
2.322) Temporal Key Integrity Protocol (TKIP) 829
2.323) Teredo 831
2.324) TOAD 833
2.325) Transmission of IP Datagrams over SMDS 836
2.326) Transport Layer Security (TLS) Protocol 839
2.327) TreeSize 841
2.328) Triple Data Encryption Algorithm (TDEA) Block Cipher 843
2.329) Unified Medical Language System (UMLS) 845
2.330) Uniform Resource Identifiers (URI) 848
2.331) Unique Ingredient Identifier (UNII) 850
2.332) United States Adopted Names (USAN) 852
2.333) United States Pharmacopeia–National Formulary (USP–NF) 854
2.334) Universal Description, Discovery, and Integration (UDDI) 856
2.335) Universal Healthcare Identifier (UHID) 860

2.336) UNIX 862
2.337) Unsolicited Email 864
2.338) User Authentication and Authorization 866
2.339) User Datagram Protocol (UDP) 868
2.340) vConverter 870
2.341) Velocity 873
2.342) Vergence Context Manager 876
2.343) Veritas Storage Foundation 879
2.344) VHIM 881
2.345) Video Codec for Audiovisual Services 886
2.346) Virtual Bridged Local Area Networks (VLAN) 888
2.347) VLAN Trunking Protocol (VTP) 890
2.348) VM Performance Toolkit 892
2.349) VMware Site Recovery Manager 894
2.350) VMware vCenter CapcityIQ 896
2.351) VMware vCenter Chargeback 898
2.352) VMware vCenter Lab Manager 900
2.353) VMware vCenter Server Heartbeat 903
2.354) VMware vSphere 905
2.355) VPN Services 907
2.356) vRanger Pro 908
2.357) Warehouse Services 911
2.358) Web Services Description Language (WSDL) 912
2.359) WebLogic Integration 916
2.360) WebLogic Portal 919
2.361) WebLogic Scripting Tool 924
2.362) WebLogic Server 926
2.363) Wide Area Network (WAN) 931
2.364) Wi-Fi Protected Access (WPA) 933
2.365) Wily Introscope 935
2.366) Windows (Client) 938
2.367) Windows (Server) 943
2.368) WinSCP 946
2.369) Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) 950

2.370) Wireless Mobile Voice 952
2.371) Wireless Transport Layer Security (WTLS) 954
2.372) Workshop for WebLogic 956
2.373) WS-Reliable Messaging 959
2.374) WS-Security 963
2.375) X.500 The Directory 966
2.376) X.509 Certificate Request Message Format (CRMF) 968
2.377) X.509 PKI Representation of Key Exchange Algorithm (KEA) Keys 970
2.378) X.509 Public Key Infrastructure (PKI) Certificate and CRL Profile 972
2.379) X.509 Public Key Infrastructure (PKI) Certificate Management Protocols 975
2.380) X.509 Public Key Infrastructure LDAP Schema 977
2.381) X.509 Public Key Infrastructure Online Certificate Status Protocol (OCSP) 979
2.382) X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP 981
2.383) X.509 Public Key Infrastructure Operational Protocols: LDAP 983
2.384) X.509 Public-Key and Attribute Certificate Frameworks 985
2.385) XDoclet 988
2.386) Xerces 991
2.387) XML Namespaces (XML-NS) 994
2.388) XML Path Language (XPath) 996
2.389) XML Pointer Framework 1000
2.390) XML Schema 1002
2.391) XML Signature Syntax and Processing (XML-Sig) 1005
2.392) XMLSpy 1007
2.393) XQuery 1011
2.394) XSL Transformations (XSLT) 1015
2.395) z/OS 1018
2.396) z/VM 1020
3) Approved Benefits Segment Technologies/Standards List 1022
4) Approved Benefits Segment Technologies/Standards Entries 1031
4.1) 7 kHz Audio-Coding within 64 kbit/s 1031
4.2) A Framework for IP Based Virtual Private Networks (VPNs) 1033
4.3) Access Control 1036
4.4) Access Control Framework 1037
4.5) Active Data Guard 1039

4.6) Advanced Encryption Standard (AES) 1041
4.7) Advanced Video Coding for Generic Audiovisual Services 1043
4.8) ANT 1046
4.9) Apache Commons 1049
4.10) Apache Struts 1053
4.11) Apache Tomcat 1059
4.12) Application Oriented Sites 1062
4.13) Architecture for IP Address Allocation with CIDR 1063
4.14) Audit Services 1065
4.15) Basic Transition Mechanisms for IPv6 Hosts Routers 1067
4.16) Biometric Application Programming Interface (BioAPI) 1069
4.17) Biometric Information Management and Security 1072
4.18) Biometric Services 1074
4.19) BMC Mainview 1076
4.20) Border Gateway Protocol (BGP) 1078
4.21) Broadband Audiovisual Communication Systems and Terminals 1080
4.22) Call Signalling Protocols and Media Stream Packetization 1082
4.23) Carrier Sense Multiple Access with Collision Detection (CSMA/CD) 1084
4.24) Cascading Style Sheets (CSS) 1087
4.25) Cascading Style Sheets Mobile Profile (CSS-Mobile) 1089
4.26) Checksum Hash Value 1091
4.27) Classless Inter-Domain Routing (CIDR) 1093
4.28) Coding of Speech Using Low-Delay Code Excited Linear Prediction 1095
4.29) Common Biometric Exchange Formats Framework (CBEFF) 1097
4.30) Common Language Infrastructure (CLI) 1099
4.31) Common Object Request Broker Architecture (CORBA) 1101
4.32) Common Warehouse Metamodel (CWM) 1104
4.33) Computer Based Training Exchange 1106
4.34) Computer Graphics Metafile (CGM) 1108
4.35) Confidentiality Framework 1110
4.36) Confidentiality Services 1112
4.37) Configuration Management 1114
4.38) Control Protocol for Multimedia Communication 1115
4.39) Cryptographic Algorithm Implementation Requirements for ESP and AH 1117

4.40) Data Center 1120
4.41) Data Encryption Standard (DES) 1122
4.42) Data Format Classification 1124
4.43) Data Format for Fingerprint, Facial, & SMT Information 1126
4.44) Data Integrity 1128
4.45) Data Oriented Sites 1130
4.46) Data Protocols for Multimedia Conferencing 1131
4.47) Data Protocols for Multimedia Conferencing - Generic Conference Control 1133
4.48) Database Services 1136
4.49) Datatypes for DTDs (DT4DTD) 1137
4.50) Differentiated Services (DS) Field in IPv4 and IPv6 Headers 1139
4.51) Digital Compression and Coding of Continuous-Tone Still Images 1141
4.52) Digital Signature 1144
4.53) Digital Signature Standard (DSS) 1145
4.54) Dimensions CM 1147
4.55) Directory Server 1149
4.56) Discovery Services 1151
4.57) Diskeeper 1153
4.58) Domain Name Service 1155
4.59) Domain Name System (DNS) Configuration Options 1157
4.60) Domain Name System (DNS) Extensions 1159
4.61) Domain Name System (DNS) Structure and Delegation 1161
4.62) Dynamic Host Configuration Protocol (DHCP) 1163
4.63) Dynamic Host Configuration Protocol Configuration of IPsec Tunnel Mode (DHCPv4) 1165
4.64) Dynamic Host Configuration Protocol for IPv6 (DHCPv6) 1167
4.65) Dynamic Server Side Display 1169
4.66) Dynamic Updates in the Domain Name System (DNS UPDATE) 1171
4.67) ebXML Collaboration Protocol Profile and Agreement (ebXML CPPA) 1173
4.68) ebXML Messaging Service (ebMS) 1176
4.69) ebXML Registry Information Model (ebRIM) 1178
4.70) ebXML Registry Services (ebRS) 1180
4.71) Eclipse 1183
4.72) Eclipse WTP 1186
4.73) eGate Integrator 1188

4.74) Encryption Algorithm and IPsec 1191
4.75) Encryption Services 1193
4.76) Enhanced Security Services for S/MIME 1194
4.77) Escrowed Encryption Standard 1197
4.78) Establishing Communication Between Multiple Audiovisual Terminals 1199
4.79) European Article Number (EAN-13) 1201
4.80) Exchange Server 1203
4.81) Extended Simple Mail Transfer Protocol (ESMTP) 1205
4.82) eXtensible Access Control Markup Language (XACML) 1207
4.83) Extensible Authentication Protocol (EAP) 1209
4.84) Extensible Authentication Protocol Tunneled Transport Layer Security (EAP-TTLS) 1211
4.85) Extensible HyperText Markup Language (XHTML) 1214
4.86) Extensible Markup Language (XML) 1216
4.87) Fault Management 1219
4.88) FDR 1221
4.89) Fiber Distributed Data Interface (FDDI) 1223
4.90) File Transfer Protocol (FTP) 1226
4.91) File Transfer Protocol (FTP) Extensions 1228
4.92) File Transfer Protocol Services 1231
4.93) FileNet P8 1232
4.94) Fire Walling 1234
4.95) Firefox 1236
4.96) Frame Structure in Audiovisual Teleservices 1239
4.97) Frame-synchronous Control and Indication Signals for Audiovisual Systems 1241
4.98) General Parallel File System (GPFS) 1243
4.99) Graphics Interchange Format (GIF) 1245
4.100) Health Information Data Exchange 1247
4.101) HyperText Markup Language (HTML) 1248
4.102) Hypertext Transfer Protocol (HTTP) 1251
4.103) Hypertext Transfer Protocol Services 1253
4.104) Identification Authentication 1254
4.105) Identification Cards - Integrated Circuit(s) Cards With Contacts 1256
4.106) Internet Control Message Protocol (ICMP) 1259
4.107) Internet Explorer 1261

4.108) Internet Key Exchange (IKE) 1264
4.109) Internet Message Access Protocol (IMAP) 1267
4.110) Internet Message Format 1269
4.111) Internet Protocol (IP) 1271
4.112) Internet Protocol Version 6 (IPv6) 1273
4.113) Internet Web 1275
4.114) Intranet Web 1276
4.115) Intrusion Detection and Prevention Systems (IDPS) 1278
4.116) Intrusion Detection Devices 1280
4.117) IP Authentication Header (AH) 1282
4.118) IP Encapsulating Security Payload (ESP) 1284
4.119) IP Network Address Translator (NAT) 1286
4.120) IP Routing Services 1288
4.121) IPsec Transport Mode for Dynamic Routing 1290
4.122) IPsec-Network Address Translation (NAT) 1292
4.123) IPv6 Client Services 1294
4.124) IPv6 over Point-to-Point Protocol (PPP) 1295
4.125) IPv6 Performance 1297
4.126) IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCPv6) 1298
4.127) IPv6/IPv4 Dual Stack Internet Access Service Model 1301
4.128) Java Data Objects (JDO) 1303
4.129) Java EE 1305
4.130) Java SE 1311
4.131) JAXB Reference Implementation 1316
4.132) JAXP Reference Implementation 1320
4.133) JPEG 1324
4.134) JPEG 2000 1326
4.135) JRules Business Rules Management Server 1329
4.136) JRules Rule Execution Server 1333
4.137) JRules Rule Studio 1336
4.138) JRules Scenario Manager 1338
4.139) JRules Team Server 1341
4.140) JUnit 1343
4.141) Key Management Using ANSI X9.17 1346

4.142) Keyed-Hash Message Authentication Code (HMAC) 1349
4.143) Layer Two Tunneling Protocol (L2TP) 1351
4.144) Lightweight EAP (LEAP) 1353
4.145) LiveCycle 1355
4.146) Local Area Network (LAN) 1357
4.147) Log4J 1360
4.148) Mail Services 1363
4.149) Malicious Code Detection 1364
4.150) Management Information Base (MIB) 1366
4.151) Media Servers 1369
4.152) Medical Device Interoperability 1370
4.153) Medical Radiology Images Exchange 1371
4.154) Metropolitan Area Network Services 1373
4.155) Mirth Connect 1374
4.156) MPEG-1 1376
4.157) MPEG-2 1379
4.158) MPEG-4 1382
4.159) Multimedia Transport 1386
4.160) Multiplexing Protocol for Low Bit Rate Multimedia Communication 1388
4.161) Multipoint Binary File Transfer Protocol 1390
4.162) Multipoint Communication Service (MCS) - Service Definition 1392
4.163) Multipoint Communication Service (MCS) Protocol 1395
4.164) Multipoint Control Units for Audiovisual Systems 1397
4.165) Multipoint Still Image and Annotation Protocol 1399
4.166) Multiprotocol Label Switching (MPLS) Architecture 1401
4.167) Multipurpose Internet Mail Extensions (MIME) 1403
4.168) Narrow-band Visual Telephone Systems and Terminal Equipment 1406
4.169) Native Audio Formats 1408
4.170) Native Document Formats 1409
4.171) Native Graphics Formats 1410
4.172) Native Video Formats 1412
4.173) Neighbor Discovery for IPv6 1413
4.174) NetBackup 1415
4.175) Network Address Translation - Protocol Translation (NAT-PT) 1417

4.176) Network Transport 1419
4.177) Network-specific Data Protocol Stacks for Multimedia Conferencing 1421
4.178) Object Linking and Embedding, Database (OLE DB) 1423
4.179) Objects and Attributes for Access Control 1425
4.180) Office Open XML 1427
4.181) Open Database Connectivity (ODBC) 1429
4.182) Open Graphics Library (OpenGL) 1432
4.183) Open Shortest Path First (OSPF) Protocol 1434
4.184) OpenVMS 1436
4.185) Oracle Database 1438
4.186) Oracle RAC 1441
4.187) Packet-Based Multimedia Communications Systems 1443
4.188) Parallel Sysplex 1446
4.189) Password Services 1448
4.190) Performance Management 1449
4.191) Pharmacological Orders Exchange 1451
4.192) PlateSpin Migrate 1452
4.193) PlateSpin PowerConvert 1455
4.194) PlateSpin Protect 1457
4.195) Point-to-Point Protocol (PPP) 1459
4.196) Portable Document Format (PDF) 1461
4.197) Portable Network Graphics (PNG) 1463
4.198) Portlet 1465
4.199) Post Office Protocol (POP) 1468
4.200) PPP Triple-DES Encryption Protocol (3DESE) 1470
4.201) Processor Area Network (PAN) Manager 1472
4.202) Protected Extensible Authentication Protocol (PEAP) 1474
4.203) Public Key Infrastructure 1476
4.204) Pulse Code Modulation (PCM) of Voice Frequencies 1479
4.205) Radio Frequency Management 1481
4.206) Rational ClearCase with MultiSite 1482
4.207) Rational Software Modeler 1486
4.208) Regulations and Procedures for Federal Radio Frequency Management 1490
4.209) Remote Access Protocol 1492

4.210) Remote Authentication Dial In User Service (RADIUS) 1493
4.211) Rich Text Format (RTF) 1495
4.212) Scalable Vector Graphics (SVG) 1497
4.213) Secure Code Design 1500
4.214) Secure Hash Standard (SHS) 1501
4.215) Secure Hypertext Transfer Protocol (S-HTTP) 1503
4.216) Secure Remote Access with L2TP 1505
4.217) Secure/Multipurpose Internet Mail Extensions (S/MIME) Certificate Handling 1507
4.218) Secure/Multipurpose Internet Mail Extensions (S/MIME) Message Spec 1509
4.219) Securing Layer Two Tunneling Protocol (L2TP) with IPsec 1511
4.220) Security Architecture for the Internet Protocol (IP) 1513
4.221) Security Architecture for the Internet Protocol (IPSec) 1515
4.222) Security Assertion Markup Language (SAML) 1517
4.223) Security Requirements for Cryptographic Modules 1520
4.224) Security Token 1522
4.225) Servers 1524
4.226) SharePoint Server 1526
4.227) Simple Mail Transfer Protocol (SMTP) 1528
4.228) Simple Network Management Protocol (SNMP) 1531
4.229) Simple Object Access Protocol (SOAP) 1533
4.230) Single Sign On 1536
4.231) Solaris 1538
4.232) Stateless Dynamic Host Configuration Protocol (DHCPv6) 1541
4.233) Static Display 1543
4.234) Storage 1545
4.235) Strobe 1547
4.236) Structured Query Language (SQL) 1549
4.237) Synchronous Optical Network (SONET) 1553
4.238) System for Establishing Communication Between Audiovisual Terminals 1556
4.239) TELNET 1558
4.240) Temporal Key Integrity Protocol (TKIP) 1560
4.241) Teredo 1562
4.242) Transmission of IP Datagrams over SMDS 1564
4.243) Transport Layer Security (TLS) Protocol 1566

4.244) TreeSize 1569
4.245) Triple Data Encryption Algorithm (TDEA) Block Cipher 1571
4.246) Uniform Resource Identifiers (URI) 1573
4.247) Universal Description, Discovery, and Integration (UDDI) 1575
4.248) Universal Healthcare Identifier (UHID) 1579
4.249) UNIX 1581
4.250) Unsolicited Email 1583
4.251) User Datagram Protocol (UDP) 1584
4.252) vConverter 1587
4.253) Veritas Storage Foundation 1589
4.254) Video Codec for Audiovisual Services 1591
4.255) Virtual Bridged Local Area Networks (VLAN) 1593
4.256) VLAN Trunking Protocol (VTP) 1595
4.257) VM Performance Toolkit 1597
4.258) VMware Site Recovery Manager 1599
4.259) VMware vCenter CapcityIQ 1601
4.260) VMware vCenter Chargeback 1603
4.261) VMware vCenter Lab Manager 1605
4.262) VMware vCenter Server Heartbeat 1607
4.263) VMware vSphere 1609
4.264) VPN Services 1612
4.265) vRanger Pro 1613
4.266) Warehouse Services 1615
4.267) Web Services Description Language (WSDL) 1616
4.268) WebLogic Server 1620
4.269) Wide Area Network (WAN) 1624
4.270) Wi-Fi Protected Access (WPA) 1627
4.271) Wily Introscope 1629
4.272) Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) 1631
4.273) Wireless Mobile Voice 1634
4.274) Wireless Transport Layer Security (WTLS) 1635
4.275) WS-Reliable Messaging 1637
4.276) WS-Security 1640
4.277) X.500 The Directory 1644

4.278) X.509 Certificate Request Message Format (CRMF) 1646
4.279) X.509 PKI Representation of Key Exchange Algorithm (KEA) Keys 1648
4.280) X.509 Public Key Infrastructure (PKI) Certificate and CRL Profile 1650
4.281) X.509 Public Key Infrastructure (PKI) Certificate Management Protocols..... 1652
4.282) X.509 Public Key Infrastructure LDAP Schema..... 1654
4.283) X.509 Public Key Infrastructure Online Certificate Status Protocol (OCSP)..... 1656
4.284) X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP..... 1658
4.285) X.509 Public Key Infrastructure Operational Protocols: LDAP 1660
4.286) X.509 Public-Key and Attribute Certificate Frameworks 1663
4.287) XML Namespaces (XML-NS) 1665
4.288) XML Path Language (XPath)..... 1667
4.289) XML Pointer Framework 1671
4.290) XML Schema..... 1673
4.291) XML Signature Syntax and Processing (XML-Sig)..... 1676
4.292) XMLSpy 1678
4.293) XQuery 1682
4.294) XSL Transformations (XSLT)..... 1686
4.295) z/OS 1689
4.296) z/VM..... 1691
5) Prohibited Technologies/Standards List 1693
6) Prohibited Technologies/Standards Entries..... 1695
6.1) Abbot Java GUI Test Framework..... 1695
6.2) AOPAlliance..... 1697
6.3) AspectJ..... 1698
6.4) Beehive 1699
6.5) Cache Objects 1701
6.6) CVS 1702
6.7) Datafile 1703
6.8) Dreamweaver..... 1705
6.9) Drools 1708
6.10) GroboUtils 1710
6.11) i-net JDBC Drivers 1712
6.12) Jakarta Object Relational Bridge..... 1713
6.13) JavaServer Faces Reference Implementation 1715

6.14) JBoss 1716
6.15) jBPM 1717
6.16) JDK - JRockit 1719
6.17) JRE - JRockit 1721
6.18) M2Eclipse 1723
6.19) Maven 1725
6.20) MediaWiki 1728
6.21) MetaHelper 1730
6.22) MySQL 1732
6.23) Oracle Data Service Integrator 1733
6.24) PDF Renderer 1735
6.25) Perforce 1737
6.26) Rational XDE Developer 1738
6.27) Rational XDE Tester 1739
6.28) TestNG 1740
6.29) TPTP 1743
6.30) Tuxedo 1745
6.31) TWiki 1746
7. Enterprise Infrastructure & Engineering Standard 1750
7.1) Enterprise Engineering IT Infrastructure LAN Standard v1.0 1750
7.2) Enterprise Engineering IT Infrastructure WAN Standard v1.0 1750
7.3) Enterprise Engineering Enterprise Server Standard v1.0 1750
7.4) Enterprise Engineering Enterprise Storage Standard v1.0 1750
7.5) Enterprise Engineering Data Center Standard v1.0 1750

DISCLAIMER: The appearance of any external hyperlink references in this document does not constitute endorsement by the Department of Veterans Affairs (VA) of this Web site or the information, products, or services contained therein. The VA does not exercise any editorial control over the information you may find at these locations. Such links are provided and are consistent with the stated purpose of this VA Intranet Service.

Purpose

The primary purpose of the Enterprise Architecture (EA) is to inform and guide the decisions of the enterprise, especially as they pertain to Information Technology (IT) investments. The Veterans Affairs (VA) Technical Reference Model (One-VA TRM) is one component within the overall EA that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain enterprise applications. Moreover, the One-VA TRM, which includes the Standards Profile and Product List, collectively serve as a technology roadmap and as a tool for supporting Office of Information & Technology (OI&T).

Use this document to determine the technical alignment of projects/programs as part of the Program Management Accountability System (PMAS) process. This site includes directions for use as well as the process for submitting new technologies to be evaluated and included in future releases of the One-VA TRM. Users can search for technologies, generate reports, review forecasts, and access release history.

Proper Use

The TRM presents lists of prospective technologies for use in the development of VA IT solutions. The lists provide guidance, with constraints, on the permissible range of technologies that a development project may select to meet project requirements. The lists are not intended to direct procurements, although reference is made, where known, to existing VA licensing.

The Approved List identifies technologies and technical standards that have been assessed and have been determined to be consistent with VA's technical approach to IT solutions. Project teams may select from the set of Approved technologies; however, approved status does not indicate the suitability or compatibility of a particular set of technologies. Each project team must consult the organizations responsible for the target development, desktop, testing and/or production environments to ensure that the intended use of the technologies is supported.

The Prohibited List identifies technologies and technical standards that should not be generally utilized in the VA. Waivers to utilize a prohibited entry may be requested when deemed necessary to address specific project requirements.

1) Approved Health Segment Technologies/Standards List

Name	Vendor	Deciding Source	Decision Process	Decision Date
7 kHz Audio-Coding within 64 kbit/s *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
A Framework for IP Based Virtual Private Networks (VPNs) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Access Control		EA	TRMSP 4.3.2	3/14/2008
Access Control Framework *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
Active Data Guard *(2)(3)*	Oracle	CDCO	CDCO 6.15.2009	6/15/2009
Active Directory *(2)*	Microsoft	ARB	TRM v2	9/17/2008
Advanced Billing Concept (ABC) *(1)*	AAIHDS	EA	TRMSP 4.3.2	3/14/2008
Advanced Encryption Standard (AES) *(1)*	NIST	EA	TRMSP 4.3.2	3/14/2008
Advanced Video Coding for Generic Audiovisual Services *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
AIX *(2)(3)*	IBM	ARB	TRM v2	9/17/2008
ANT *(2)*	ASF	ARB	TRM v2	9/17/2008
Apache Cactus *(2)*	ASF	ARB	TRM v2	9/17/2008
Apache Commons *(2)*	ASF	ARB	TRM v3	1/7/2009
Apache HTTP Server *(2)(3)*	ASF	ARB	TRM v3.2	8/19/2009
Apache POI *(2)*	ASF	ARB	TRM v4	9/16/2009
Apache Struts *(2)(3)*	ASF	ARB	TRM v2	9/17/2008
Apache Tomcat *(2)(3)*	ASF	CDCO	CDCO 6.15.2009	6/15/2009
Application Oriented Sites		EA	TRMSP 4.3.2	3/14/2008
Architecture for IP Address Allocation with CIDR *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Audit Services		EA	TRMSP 4.3.2	3/14/2008
Basic Transition Mechanisms for IPv6 Hosts Routers *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Bing Maps *(2)*	Microsoft	ARB	TRM v3.2	8/19/2009
Biometric Application Programming Interface (BioAPI) *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
Biometric Information Management and Security *(1)*	ANSI	EA	TRMSP 4.3.2	3/14/2008
Biometric Services		EA	TRMSP 4.3.2	3/14/2008
BIRT *(2)*	Eclipse	ARB	TRM v3.2	8/19/2009
BlazeDS *(2)*	Adobe	ARB	TRM v4.1	10/28/2009
BMC Mainview *(2)(3)*	BMC Software	CDCO	CDCO 6.15.2009	6/15/2009
BMC Performance Manager *(2)*	BMC Software	ARB	TRM v2	9/17/2008
Bobby *(2)(3)*	Watchfire	ARB	TRM v2	9/17/2008

Border Gateway Protocol (BGP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Broadband Audiovisual Communication Systems and Terminals *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
BusinessWare *(2)*	Vitria	ARB	TRM v2	9/17/2008
Cache Database Engine *(2)*	InterSystems	ARB	TRM v2	9/17/2008
Cache JDBC Driver *(2)*	InterSystems	HSD&D	ETL	12/1/2006
Call Signalling Protocols and Media Stream Packetization *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Carrier Sense Multiple Access with Collision Detection (CSMA/CD) *(1)*	IEEE	EA	TRMSP 4.3.2	3/14/2008
Cascading Style Sheets (CSS) *(1)*	W3C	EA	TRMSP 4.3.2	3/14/2008
Cascading Style Sheets Mobile Profile (CSS-Mobile) *(1)*	W3C	EA	TRMSP 4.3.2	3/14/2008
Castor XML *(2)*	Castor	HSD&D	ETL	12/1/2006
Checksum Hash Value		EA	TRMSP 4.3.2	3/14/2008
Classless Inter-Domain Routing (CIDR) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Coding of Speech Using Low-Delay Code Excited Linear Prediction *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Common Biometric Exchange Formats Framework (CBEFF) *(1)*	NIST	EA	TRMSP 4.3.2	3/14/2008
Common Language Infrastructure (CLI) *(1)*	ECMA	EA	TRMSP 4.3.2	3/14/2008
Common Object Request Broker Architecture (CORBA) *(1)*	OASIS	EA	TRMSP 4.3.2	3/14/2008
Common Warehouse Metamodel (CWM) *(1)*	OMG	EA	TRMSP 4.3.2	3/14/2008
Computer Based Training Exchange		EA	TRMSP 4.3.2	3/14/2008
Computer Graphics Metafile (CGM) *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
Confidentiality Framework *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
Confidentiality Services		EA	TRMSP 4.3.2	3/14/2008
Configuration Management		EA	TRMSP 4.3.2	3/14/2008
Control Protocol for Multimedia Communication *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Cryptographic Algorithm Implementation Requirements for ESP and AH *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Current Dental Terminology (CDT) *(1)*	ADA	EA	TRMSP 4.3.2	3/14/2008
Current Procedural Terminology (CPT) *(1)*	AMA	EA	TRMSP 4.3.2	3/14/2008
Data Center *(1)*		EIE CTO	TAR-TAS	11/13/2009
Data Encryption Standard (DES) *(1)*	NIST	EA	TRMSP 4.3.2	3/14/2008
Data Format Classification		EA	TRMSP 4.3.2	3/14/2008
Data Format for Fingerprint, Facial, & SMT Information *(1)*	NIST	EA	TRMSP 4.3.2	3/14/2008
Data Integrity		EA	TRMSP 4.3.2	3/14/2008

Data Oriented Sites		EA	TRMSP 4.3.2	3/14/2008
Data Protocols for Multimedia Conferencing *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Data Protocols for Multimedia Conferencing - Generic Conference Control *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Database Services		EA	TRMSP 4.3.2	3/14/2008
Datatypes for DTDs (DT4DTD) *(1)*	W3C	EA	TRMSP 4.3.2	3/14/2008
Datejs *(2)*	Google	ARB	TRM v3.2	8/19/2009
Diagnosis-Related Group (DRG) *(1)*	CMS	EA	TRMSP 4.3.2	3/14/2008
Diagnostic and Statistical Manual of Mental Disorders (DSM) *(1)*	APA	EA	TRMSP 4.3.2	3/14/2008
Differentiated Services (DS) Field in IPv4 and IPv6 Headers *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Digital Compression and Coding of Continuous-Tone Still Images *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
Digital Imaging and Communications in Medicine (DICOM) *(1)*	NEMA	EA	TRMSP 4.3.2	3/14/2008
Digital Signature		EA	TRMSP 4.3.2	3/14/2008
Digital Signature Standard (DSS) *(1)*	NIST	EA	TRMSP 4.3.2	3/14/2008
Directory Server *(2)(3)*	Oracle	CDCO	CDCO 6.15.2009	6/15/2009
Discovery Services		EA	TRMSP 4.3.2	3/14/2008
Diskeeper *(2)(3)*	Diskeeper Corp.	CDCO	CDCO 6.15.2009	6/15/2009
Domain Name Service		EA	TRMSP 4.3.2	3/14/2008
Domain Name System (DNS) Configuration Options *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Domain Name System (DNS) Extensions *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Domain Name System (DNS) Structure and Delegation *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Dynamic Host Configuration Protocol (DHCP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Dynamic Host Configuration Protocol Configuration of IPsec Tunnel Mode (DHCPv4) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Dynamic Host Configuration Protocol for IPv6 (DHCPv6) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Dynamic Server Side Display		EA	TRMSP 4.3.2	3/14/2008
Dynamic Updates in the Domain Name System (DNS UPDATE) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
ebXML Collaboration Protocol Profile and Agreement (ebXML CPPA) *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
ebXML Messaging Service (ebMS) *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
ebXML Registry Information Model (ebRIM) *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
ebXML Registry Services (ebRS) *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
Eclipse *(2)*	Eclipse	ARB	TRM v2	9/17/2008

Eclipse Modeling Framework (EMF) *(2)*	Eclipse	ARB	TRM v3.2	8/19/2009
eGate Integrator *(2)(3)*	Oracle	CDCO	CDCO 6.15.2009	6/15/2009
Electronic Authentication of Health Care Information *(1)*	ASTM	EA	TRMSP 4.3.2	3/14/2008
Encryption Algorithm and IPsec *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Encryption Services		EA	TRMSP 4.3.2	3/14/2008
Enhanced Security Services for S/MIME *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Environmental Protection Agency - Substance Registry System (EPA-SRS) *(1)*	EPA	EA	TRMSP 4.3.2	3/14/2008
ERwin Data Modeler *(2)*	CA	HSD&D	ETL	12/1/2006
Escrowed Encryption Standard *(1)*	NIST	EA	TRMSP 4.3.2	3/14/2008
Establishing Communication Between Multiple Audiovisual Terminals *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
European Article Number (EAN-13) *(1)*	GS1	EA	TRMSP 4.3.2	3/14/2008
Exchange Server *(2)(3)*	Microsoft	CDCO	CDCO 6.15.2009	6/15/2009
Extended Simple Mail Transfer Protocol (ESMTP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
eXtensible Access Control Markup Language (XACML) *(1)*	OASIS	EA	TRMSP 4.3.2	3/14/2008
Extensible Authentication Protocol (EAP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Extensible Authentication Protocol Tunneled Transport Layer Security (EAP-TTLS) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Extensible HyperText Markup Language (XHTML) *(1)*	W3C	EA	TRMSP 4.3.2	3/14/2008
Extensible Markup Language (XML) *(1)*	W3C	Benefits Arch	TRM v4.1	10/28/2009
Fault Management		EA	TRMSP 4.3.2	3/14/2008
FDR *(2)(3)*	Innovation	CDCO	CDCO 6.15.2009	6/15/2009
Fiber Distributed Data Interface (FDDI) *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
File Transfer Protocol (FTP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
File Transfer Protocol (FTP) Extensions *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
File Transfer Protocol Services		EA	TRMSP 4.3.2	3/14/2008
Fire Walling		EA	TRMSP 4.3.2	3/14/2008
Firefox *(2)*	Mozilla	ARB	TRM v2	9/17/2008
Flex SDK *(2)*	Adobe	ARB	TRM v4.1	10/28/2009
Frame Structure in Audiovisual Teleservices *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Frame-synchronous Control and Indication Signals for Audiovisual Systems *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
General Parallel File System (GPFS) *(2)(3)*	IBM	CDCO	CDCO 6.15.2009	6/15/2009
Google Maps *(2)*	Google	ARB	TRM v3.2	8/19/2009
Graphics Interchange Format (GIF) *(1)*	W3C	EA	TRMSP 4.3.2	3/14/2008
Health Information Data Exchange		EA	TRMSP 4.3.2	3/14/2008

Healthcare Common Procedure Coding System (HCPCS) *(1)*	CMS	EA	TRMSP 4.3.2	3/14/2008
Hibernate Core *(2)*	RedHat	ARB	TRM v2	9/17/2008
HL7 *(1)*	HL7	ARB	TRM v2	9/17/2008
HP-UX *(2)(3)*	HP	ARB	TRM v2	9/17/2008
Human Gene Nomenclature (HGN) *(1)*	HUGO	EA	TRMSP 4.3.2	3/14/2008
HyperText Markup Language (HTML) *(1)*	W3C	EA	TRMSP 4.3.2	3/14/2008
Hypertext Transfer Protocol (HTTP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Hypertext Transfer Protocol Services		EA	TRMSP 4.3.2	3/14/2008
Identification Authentication		EA	TRMSP 4.3.2	3/14/2008
Identification Cards - Integrated Circuit(s) Cards With Contacts *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
ImageGear *(2)*	Accusoft Pegasus	ARB	TRM v4.1	10/28/2009
Information Access Privileges to Health Information *(1)*	ASTM	EA	TRMSP 4.3.2	3/14/2008
InfoSphere Data Architect *(2)(3)*	IBM	ARB	TRM v4	9/16/2009
InstallShield *(2)*	Acresso	ARB	TRM v2	9/17/2008
International Classification of Diseases (ICD) *(1)*	N/A	EA	TRMSP 4.3.2	3/14/2008
International Nonproprietary Names (INN) *(1)*	WHO	EA	TRMSP 4.3.2	3/14/2008
Internet Control Message Protocol (ICMP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Internet Explorer *(2)*	Microsoft	ARB	TRM v2	9/17/2008
Internet Information Services (IIS) *(2)*	Microsoft	ARB	TRM v3.2	8/19/2009
Internet Key Exchange (IKE) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Internet Message Access Protocol (IMAP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Internet Message Format *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Internet Protocol (IP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Internet Protocol Version 6 (IPv6) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Internet Web		EA	TRMSP 4.3.2	3/14/2008
Intranet Web		EA	TRMSP 4.3.2	3/14/2008
Intrusion Detection and Prevention Systems (IDPS) *(1)*	NIST	EA	TRMSP 4.3.2	3/14/2008
Intrusion Detection Devices		EA	TRMSP 4.3.2	3/14/2008
IP Authentication Header (AH) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
IP Encapsulating Security Payload (ESP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
IP Network Address Translator (NAT) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
IP Routing Services*(3)*		EA	TRMSP 4.3.2	3/14/2008
IPsec Transport Mode for Dynamic Routing *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
IPsec-Network Address Translation (NAT) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
IPv6 Client Services		EA	TRMSP 4.3.2	3/14/2008
IPv6 over Point-to-Point Protocol (PPP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008

IPv6 Performance		EA	TRMSP 4.3.2	3/14/2008
IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCPv6) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
IPv6/IPv4 Dual Stack Internet Access Service Model *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
iText Core *(2)*	N/A	ARB	TRM v4	9/16/2009
Java AVK *(2)*	Sun Microsystems	ARB	TRM v2	9/17/2008
Java Data Objects (JDO) *(1)*	Sun Microsystems	EA	TRMSP 4.3.2	3/14/2008
Java EE *(1)*	Sun Microsystems	ARB	TRM v2	9/17/2008
Java SE *(1)*	Sun Microsystems	ARB	TRM v2	9/17/2008
JavaScript *(1)*	ECMA	ARB	TRM v3	1/7/2009
JAWS *(2)*	Freedom Scientific	ARB	TRM v2	9/17/2008
JAXB Reference Implementation *(2)*	Sun Microsystems	ARB	TRM v2	9/17/2008
JAXP Reference Implementation *(2)*	Sun Microsystems	ARB	TRM v2	9/17/2008
JPEG *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
JPEG 2000 *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
JProbe *(2)*	Quest Software	ARB	TRM v2	9/17/2008
JRules Business Rules Management Server *(2)*	ILOG	ARB	TRM v3.1	5/13/2009
JRules Rule Execution Server *(2)*	ILOG	ARB	TRM v3.1	5/13/2009
JRules Rule Studio *(2)*	ILOG	ARB	TRM v3.1	5/13/2009
JRules Scenario Manager *(2)*	ILOG	ARB	TRM v3.1	5/13/2009
JRules Team Server *(2)*	ILOG	ARB	TRM v3.1	5/13/2009
JUnit *(2)*	SourceForge	ARB	TRM v2	9/17/2008
Key Management Using ANSI X9.17 *(1)*	NIST	EA	TRMSP 4.3.2	3/14/2008
Keyed-Hash Message Authentication Code (HMAC) *(1)*	NIST	EA	TRMSP 4.3.2	3/14/2008
Layer Two Tunneling Protocol (L2TP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Lightweight Directory Access Protocol (LDAP) *(1)*	IETF	ARB	TRM v2	9/17/2008
Lightweight EAP (LEAP) *(1)*		EA	TRMSP 4.3.2	3/14/2008
Local Area Network (LAN) *(1)*		EIE CTO	TAR-TAS	11/5/2009
Log4J *(2)*	ASF	ARB	TRM v2	9/17/2008
Logical Observation Identifiers Names and Codes (LOINC) *(1)*	LOINC	EA	TRMSP 4.3.2	3/14/2008
Mail Services		EA	TRMSP 4.3.2	3/14/2008
Malicious Code Detection		EA	TRMSP 4.3.2	3/14/2008
Management Information Base (MIB) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Media Servers		EA	TRMSP 4.3.2	3/14/2008
Medical Device Communications *(1)*	IEEE	EA	TRMSP 4.3.2	3/14/2008

Medical Device Interoperability		EA	TRMSP 4.3.2	3/14/2008
Medical Radiology Images Exchange		EA	TRMSP 4.3.2	3/14/2008
Mercury LoadRunner *(2)(3)*	HP	ARB	TRM v2	9/17/2008
Mercury WinRunner *(2)(3)*	HP	ARB	TRM v2	9/17/2008
Messaging Workbench (MWB) *(2)*	HL7	ARB	TRM v3.2	8/19/2009
Metropolitan Area Network Services		EA	TRMSP 4.3.2	3/14/2008
Mirth Connect *(2)(3)*	Mirth Corp.	CDCO	CDCO 6.15.2009	6/15/2009
MPEG-1 *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
MPEG-2 *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
MPEG-4 *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
Multimedia Transport*(3)*		EA	TRMSP 4.3.2	3/14/2008
Multiplexing Protocol for Low Bit Rate Multimedia Communication *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Multipoint Binary File Transfer Protocol *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Multipoint Communication Service (MCS) - Service Definition *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Multipoint Communication Service (MCS) Protocol *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Multipoint Control Units for Audiovisual Systems *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Multipoint Still Image and Annotation Protocol *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Multiprotocol Label Switching (MPLS) Architecture *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Multipurpose Internet Mail Extensions (MIME) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
MyEclipse *(2)*	Genuitec	ARB	TRM v2	9/17/2008
Narrow-band Visual Telephone Systems and Terminal Equipment *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
National Cancer Institute Thesaurus (NCIt) *(1)*	NCI	EA	TRMSP 4.3.2	3/14/2008
National Drug Code (NDC) *(1)*	N/A	EA	TRMSP 4.3.2	3/14/2008
National Drug File – Reference Terminology (NDF-RT) *(1)*	N/A	EA	TRMSP 4.3.2	3/14/2008
Native Audio Formats		EA	TRMSP 4.3.2	3/14/2008
Native Document Formats		EA	TRMSP 4.3.2	3/14/2008
Native Graphics Formats		EA	TRMSP 4.3.2	3/14/2008
Native Video Formats		EA	TRMSP 4.3.2	3/14/2008
NCPDP Telecommunication Standards *(1)*	NCPDP	EA	TRMSP 4.3.2	3/14/2008
Neighbor Discovery for IPv6 *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
NetBackup *(2)(3)*	Symantec	CDCO	CDCO 6.15.2009	6/15/2009
Network Address Translation - Protocol Translation (NAT-PT) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Network Transport		EA	TRMSP 4.3.2	3/14/2008

Network-specific Data Protocol Stacks for Multimedia Conferencing *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Object Linking and Embedding, Database (OLE DB) *(1)*	Microsoft	EA	TRMSP 4.3.2	3/14/2008
Objects and Attributes for Access Control *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
Office Open XML *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
Open Database Connectivity (ODBC) *(1)*	Microsoft	EA	TRMSP 4.3.2	3/14/2008
Open Graphics Library (OpenGL) *(1)*	OpenGL	EA	TRMSP 4.3.2	3/14/2008
Open Shortest Path First (OSPF) Protocol *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
OpenVMS *(2)(3)*	HP	CDCO	CDCO 6.15.2009	6/15/2009
Oracle Database *(2)(3)*	Oracle	ARB	TRM v2	9/17/2008
Oracle JDBC Drivers *(2)*	Oracle	ARB	TRM v2	9/17/2008
Packet-Based Multimedia Communications Systems *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Parallel Sysplex *(2)(3)*	IBM	CDCO	CDCO 6.15.2009	6/15/2009
Password Services		EA	TRMSP 4.3.2	3/14/2008
Performance Management		EA	TRMSP 4.3.2	3/14/2008
Person Identification Service (PIDS) *(1)*	OMG	EA	TRMSP 4.3.2	3/14/2008
Pharmacological Orders Exchange		EA	TRMSP 4.3.2	3/14/2008
PlateSpin Migrate *(2)(3)*	Novell	CDCO	CDCO 6.15.2009	6/15/2009
PlateSpin PowerConvert *(2)(3)*	Novell	CDCO	CDCO 6.15.2009	6/15/2009
PlateSpin Protect *(2)(3)*	Novell	CDCO	CDCO 6.15.2009	6/15/2009
Point-of-care Medical Device Communication *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
Point-to-Point Protocol (PPP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Portable Document Format (PDF) *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
Portable Network Graphics (PNG) *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
Portlet *(1)*	Sun Microsystems	EA	TRMSP 4.3.2	3/14/2008
Post Office Protocol (POP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
PPP Triple-DES Encryption Protocol (3DESE) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Primavera TeamPlay *(2)*	Oracle	HSD&D	ETL	12/1/2006
Processor Area Network (PAN) Manager *(2)(3)*	Egenera	CDCO	CDCO 6.15.2009	6/15/2009
Protected Extensible Authentication Protocol (PEAP) *(1)*	Microsoft	EA	TRMSP 4.3.2	3/14/2008
Public Key Infrastructure		EA	TRMSP 4.3.2	3/14/2008
Pulse Code Modulation (PCM) of Voice Frequencies *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Radio Frequency Management		EA	TRMSP 4.3.2	3/14/2008
Rational Asset Manager *(2)(3)*	IBM	ARB	TRM v4	9/16/2009
Rational Build Forge *(2)(3)*	IBM	ARB	TRM v3	1/7/2009

Rational ClearCase with MultiSite *(2)(3)*	IBM	ARB	TRM v2	9/17/2008
Rational ClearQuest with MultiSite *(2)(3)*	IBM	ARB	TRM v2	9/17/2008
Rational Functional Tester *(2)(3)*	IBM	ARB	TRM v2	9/17/2008
Rational Manual Tester *(2)(3)*	IBM	ARB	TRM v2	9/17/2008
Rational Performance Tester *(2)(3)*	IBM	ARB	TRM v4	9/16/2009
Rational PurifyPlus *(2)(3)*	IBM	HSD&D	ETL	12/1/2006
Rational Quality Manager *(2)(3)*	IBM	ARB	TRM v4	9/16/2009
Rational Requirements Composer *(2)(3)*	IBM	ARB	TRM v4	9/16/2009
Rational RequisitePro *(2)(3)*	IBM	ARB	TRM v2	9/17/2008
Rational Robot *(2)(3)*	IBM	HSD&D	ETL	12/1/2006
Rational Rose *(2)(3)*	IBM	HSD&D	ETL	12/1/2006
Rational RUP *(2)(3)*	IBM	HSD&D	ETL	12/1/2006
Rational Software Architect *(2)(3)*	IBM	ARB	TRM v2	9/17/2008
Rational Software Modeler *(2)(3)*	IBM	ARB	TRM v2	9/17/2008
Rational Team Concert *(2)(3)*	IBM	ARB	TRM v3.2	8/19/2009
Rational TestFactory *(2)(3)*	IBM	HSD&D	ETL	12/1/2006
Rational TestManager *(2)(3)*	IBM	ARB	TRM v2	9/17/2008
Red Hat Linux *(2)*	RedHat	ARB	TRM v2	9/17/2008
Reflections *(2)*	Attachmate	ARB	TRM v4	9/16/2009
Regulations and Procedures for Federal Radio Frequency Management *(1)*	NTIA	EA	TRMSP 4.3.2	3/14/2008
Remote Access Protocol		EA	TRMSP 4.3.2	3/14/2008
Remote Authentication Dial In User Service (RADIUS) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Resource-Based Relative Value Scale (RBRVS) *(1)*	AMA	EA	TRMSP 4.3.2	3/14/2008
Rich Text Format (RTF) *(1)*	Microsoft	EA	TRMSP 4.3.2	3/14/2008
RoboHelp *(2)*	Adobe	ARB	TRM v3	1/7/2009
RxNorm *(1)*	NIH	EA	TRMSP 4.3.2	3/14/2008
Scalable Vector Graphics (SVG) *(1)*	W3C	EA	TRMSP 4.3.2	3/14/2008
Secure Code Design		EA	TRMSP 4.3.2	3/14/2008
Secure Hash Standard (SHS) *(1)*	NIST	EA	TRMSP 4.3.2	3/14/2008
Secure Hypertext Transfer Protocol (S-HTTP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Secure Remote Access with L2TP *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Secure/Multipurpose Internet Mail Extensions (S/MIME) Certificate Handling *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Secure/Multipurpose Internet Mail Extensions (S/MIME) Message Spec *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Securing Layer Two Tunneling Protocol (L2TP) with IPsec *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008

Security Architecture for the Internet Protocol (IP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Security Architecture for the Internet Protocol (IPSec) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Security Assertion Markup Language (SAML) *(1)*	OASIS	Benefits Arch	TRM v4.1	10/28/2009
Security Requirements for Cryptographic Modules *(1)*	NIST	EA	TRMSP 4.3.2	3/14/2008
Security Token		EA	TRMSP 4.3.2	3/14/2008
Servers *(1)*		EIE CTO	TAR-TAS	11/18/2009
SharePoint Server *(2)(3)*	Microsoft	CDCO	CDCO 6.15.2009	6/15/2009
Simple Mail Transfer Protocol (SMTP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Simple Network Management Protocol (SNMP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Simple Object Access Protocol (SOAP) *(1)*	W3C	Benefits Arch	TRM v4.1	10/28/2009
Single Sign On		EA	TRMSP 4.3.2	3/14/2008
SiteMinder Web Access Manager *(2)*	CA	ARB	TRM v4	9/16/2009
Solaris *(2)(3)*	Sun Microsystems	ARB	TRM v2	9/17/2008
Spring Framework *(2)*	SpringSource	ARB	TRM v3	1/7/2009
Spry Framework *(2)*	Adobe	ARB	TRM v3.2	8/19/2009
SQL Server *(2)*	Microsoft	ARB	TRM v3	1/7/2009
Stateless Dynamic Host Configuration Protocol (DHCPv6) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Static Display		EA	TRMSP 4.3.2	3/14/2008
Storage *(1)*		EIE CTO	TAR-TAS	11/18/2009
Strobe *(1)(3)*	Compuware	CDCO	CDCO 6.15.2009	6/15/2009
Structured Query Language (SQL) *(1)*	ANSI	Benefits Arch	TRM v4.1	10/28/2009
Synchronous Optical Network (SONET) *(1)*	ANSI	EA	TRMSP 4.3.2	3/14/2008
System for Establishing Communication Between Audiovisual Terminals *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Systematized Nomenclature of Medicine-Clinical Terms (SNOMED CT) *(1)*	IHTSDO	EA	TRMSP 4.3.2	3/14/2008
TeamPage *(2)*	Traction Software	ARB	TRM v3.2	8/19/2009
TELNET *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Temporal Key Integrity Protocol (TKIP) *(1)*	IEEE	EA	TRMSP 4.3.2	3/14/2008
Teredo *(1)(3)*	Microsoft	CDCO	CDCO 6.15.2009	6/15/2009
TOAD *(2)*	Quest Software	ARB	TRM v2	9/17/2008
Transmission of IP Datagrams over SMDS *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Transport Layer Security (TLS) Protocol *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
TreeSize *(2)(3)*	JAM Software	CDCO	CDCO 6.15.2009	6/15/2009
Triple Data Encryption Algorithm (TDEA) Block Cipher *(1)*	NIST	EA	TRMSP 4.3.2	3/14/2008
Unified Medical Language System (UMLS) *(2)*	NIH	EA	TRMSP 4.3.2	3/14/2008

Uniform Resource Identifiers (URI) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Unique Ingredient Identifier (UNII) *(1)*	FDA	EA	TRMSP 4.3.2	3/14/2008
United States Adopted Names (USAN) *(1)*	AMA	EA	TRMSP 4.3.2	3/14/2008
United States Pharmacopeia–National Formulary (USP–NF) *(1)*	U.S. Pharmacopeia	EA	TRMSP 4.3.2	3/14/2008
Universal Description, Discovery, and Integration (UDDI) *(1)*	OASIS	Benefits Arch	TRM v4.1	10/28/2009
Universal Healthcare Identifier (UHID) *(1)*	ASTM	EA	TRMSP 4.3.2	3/14/2008
UNIX *(1)*	The Open Group	EA	TRMSP 4.3.2	3/14/2008
Unsolicited Email		EA	TRMSP 4.3.2	3/14/2008
User Authentication and Authorization *(1)*	ASTM	EA	TRMSP 4.3.2	3/14/2008
User Datagram Protocol (UDP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
vConverter *(2)(3)*	Quest Software	CDCO	CDCO 6.15.2009	6/15/2009
Velocity *(2)*	ASF	ARB	TRM v3.2	8/19/2009
Vergence Context Manager *(2)*	Sentillion	ARB	TRM v2	9/17/2008
Veritas Storage Foundation *(2)(3)*	Symantec	CDCO	CDCO 6.15.2009	6/15/2009
VHIM *(2)*	N/A	ARB	TRM v2	9/17/2008
Video Codec for Audiovisual Services *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Virtual Bridged Local Area Networks (VLAN) *(1)*	IEEE	EA	TRMSP 4.3.2	3/14/2008
VLAN Trunking Protocol (VTP) *(1)*	Cisco	EA	TRMSP 4.3.2	3/14/2008
VM Performance Toolkit *(2)(3)*	IBM	CDCO	CDCO 6.15.2009	6/15/2009
VMware Site Recovery Manager *(2)(3)*	VMware	CDCO	CDCO 6.15.2009	6/15/2009
VMware vCenter CapcityIQ *(2)(3)*	VMware	CDCO	CDCO 6.15.2009	6/15/2009
VMware vCenter Chargeback *(2)(3)*	VMware	CDCO	CDCO 6.15.2009	6/15/2009
VMware vCenter Lab Manager *(2)(3)*	VMware	CDCO	CDCO 6.15.2009	6/15/2009
VMware vCenter Server Heartbeat *(2)(3)*	VMware	CDCO	CDCO 6.15.2009	6/15/2009
VMware vSphere *(2)(3)*	VMware	CDCO	CDCO 6.15.2009	6/15/2009
VPN Services		EA	TRMSP 4.3.2	3/14/2008
vRanger Pro *(2)(3)*	Quest Software	CDCO	CDCO 6.15.2009	6/15/2009
Warehouse Services		EA	TRMSP 4.3.2	3/14/2008
Web Services Description Language (WSDL) *(1)*	W3C	ARB	TRM v2	9/17/2008
WebLogic Integration *(2)*	Oracle	ARB	TRM v3.1	5/13/2009
WebLogic Portal *(2)*	Oracle	ARB	TRM v3.1	5/13/2009
WebLogic Scripting Tool *(2)*	Oracle	ARB	TRM v3.2	8/19/2009
WebLogic Server *(2)*	Oracle	ARB	TRM v2	9/17/2008
Wide Area Network (WAN) *(1)*		EIE CTO	TAR-TAS	11/30/2009
Wi-Fi Protected Access (WPA) *(1)*	Wi-Fi Alliance	EA	TRMSP 4.3.2	3/14/2008
Wily Introscope *(2)(3)*	CA	CDCO	CDCO 6.15.2009	6/15/2009

Windows (Client) *(2)*	Microsoft	ARB	TRM v2	9/17/2008
Windows (Server) *(2)*	Microsoft	ARB	TRM v2	9/17/2008
WinSCP *(2)*	SourceForge	ARB	TRM v3	1/7/2009
Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) *(1)*	IEEE	EA	TRMSP 4.3.2	3/14/2008
Wireless Mobile Voice		EA	TRMSP 4.3.2	3/14/2008
Wireless Transport Layer Security (WTLS) *(1)*	OMA	EA	TRMSP 4.3.2	3/14/2008
Workshop for WebLogic *(2)*	Oracle	ARB	TRM v3.1	5/13/2009
WS-Reliable Messaging *(1)*	OASIS	Benefits Arch	TRM v4.1	10/28/2009
WS-Security *(1)*	OASIS	Benefits Arch	TRM v4.1	10/28/2009
X.500 The Directory *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
X.509 Certificate Request Message Format (CRMF) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
X.509 PKI Representation of Key Exchange Algorithm (KEA) Keys *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
X.509 Public Key Infrastructure (PKI) Certificate and CRL Profile *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
X.509 Public Key Infrastructure (PKI) Certificate Management Protocols *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
X.509 Public Key Infrastructure LDAP Schema *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
X.509 Public Key Infrastructure Online Certificate Status Protocol (OCSP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
X.509 Public Key Infrastructure Operational Protocols: LDAP *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
X.509 Public-Key and Attribute Certificate Frameworks *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
XDoclet *(2)*	CodeHaus	ARB	TRM v2	9/17/2008
Xerces *(2)*	ASF	ARB	TRM v3.2	8/19/2009
XML Namespaces (XML-NS) *(1)*	W3C	EA	TRMSP 4.3.2	3/14/2008
XML Path Language (XPath) *(1)*	W3C	EA	TRMSP 4.3.2	3/14/2008
XML Pointer Framework *(1)*	W3C	EA	TRMSP 4.3.2	3/14/2008
XML Schema *(1)*	W3C	EA	TRMSP 4.3.2	3/14/2008
XML Signature Syntax and Processing (XML-Sig) *(1)*	W3C	EA	TRMSP 4.3.2	3/14/2008
XMLSpy *(2)*	Altova	ARB	TRM v3.1	5/13/2009
XQuery *(1)*	W3C	Benefits Arch	TRM v4.1	10/28/2009
XSL Transformations (XSLT) *(1)*	W3C	Benefits Arch	TRM v4.1	10/28/2009
z/OS *(2)(3)*	IBM	CDCO	CDCO 6.15.2009	6/15/2009
z/VM *(2)(3)*	IBM	CDCO	CDCO 6.15.2009	6/15/2009

(1) - Indicates a standard or specification. It is in no way an endorsement or approval for technologies that implement the standard or specification.

(2) - Indicates a technology.

(3) - Indicates a constraint.

2) Approved Health Segment Technologies/Standards Entries

2.1) 7 kHz Audio-Coding within 64 kbit/s

General Information

Website:	http://www.itu.int/itu-t/recommendations/index.aspx?ser=G
Description:	ITU-T G.722: 7 kHz Audio-Coding within 64 kbit/s describes the characteristics of an audio (50 to 7,000 Hz) coding system which may be used for a variety of higher quality speech applications. The coding system uses sub-band adaptive differential pulse code modulation (SB-ADPCM) within a bit rate of 64 kbit/s.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.3	11/24/2006		
1.4	11/24/2006		
1.5	7/6/2007		
1.6	11/6/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or

production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.4	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.2) A Framework for IP Based Virtual Private Networks (VPNs)

General Information

Website: http://tools.ietf.org/html/rfc2764

Description: A Framework for IP Based Virtual Private Networks (VPNs) describes a framework for VPNs running across IP backbones. It discusses the various different types of VPNs, their respective requirements, and proposes specific mechanisms that could be used to implement each type of VPN using existing or proposed specifications. The objective of this document is to serve as a framework for related protocol development in order to develop the full set of specifications required for widespread deployment of interoperable VPN solutions.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2764	2/1/2000		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2764	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.3) Access Control

General Information

Description: Access control services prevent the unauthorized use of information system resources. These services may be applied to various aspects of access to a resource (e.g., access to communications with the resource; the reading, writing; or deletion of an information or data resource; or the execution of a processing resource) or to all accesses to a resource.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Scope		Access Controls will be applied according to VA Handbook 6500: Cyber Security and IETF RFC 2196: Site Security Handbook for services like TELNET, CGI, and FTP, which may access VA protected servers.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Access Services	Authorized system administrators should be the only ones allowed to perform access services like telnet and rlogin.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.4) Access Control Framework

General Information

Website:	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18199
Description:	ISO/IEC 10181-3: Access Control Framework specifies a general framework for the provision of access control. The purpose of access control is to counter the threat of unauthorized operations involving a computer or communication system.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code

Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1996	1/1/1996		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1996	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo

	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.5) Active Data Guard

General Information

Website:	http://www.oracle.com/technology/deploy/availability/htdocs/DataGuardOverview.html
Description:	Active Data Guard provides the management, monitoring, and automation software to create and maintain one or more synchronized replicas (standby databases) of a production database (primary database). An Active Data Guard standby database is an exact copy of the primary that is open read-only while it continuously applies changes transmitted by the primary database.
Decision:	Approved
Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	Oracle

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Database/Storage	875: Database

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- Oracle Database - ***(required libraries)***
- Oracle RAC - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Transmission Control Protocol (TCP) related as: (Companion)
- Internet Protocol (IP) related as: (Companion)
- Structured Query Language (SQL) related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the

responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	See Oracle Database for Release and VA Forecast information.

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.6) Active Directory

General Information

Website:	http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx
Description:	Active Directory (AD) is an implementation of Lightweight Directory Access Protocol (LDAP) directory services by Microsoft for use primarily in Windows environments. The main purpose of Active Directory is to provide central authentication and authorization services for Windows based computers. Active Directory also allows administrators to assign policies, deploy software, and apply critical updates to an entire organization. Active Directory stores information and settings relating to an organization in a central, organized, accessible database. Active Directory networks can vary from a small installation with a few hundred objects, to a large installation with millions of objects.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2

Decision Date: 9/17/2008
Current Status: Analysis Completed
Introduced By: TRM Team
Vendor Name: Microsoft

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	885: Supporting Security Services

Operating Systems Supported

- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Windows (Server) - ***(required libraries)***

Comparable Technologies/Standards:

- Lightweight Directory Access Protocol (LDAP)

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (10/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	Please refer to the Windows Server entry for VA Forecast Information

General Analysis

Architectural Area

- Integration

Architectural Benefits

- Software Restriction Policies
- Integration

Tool Type

- Platform

Tool Usage

- Runtime

General Assessment

Expected Usage: Provides central authentication and authorization services for Windows based systems.

Assessment Type:	Refresh
Assessment Date:	11/19/2008
Notes:	Active Directory is not released individually--but WITH releases of the Windows server operating system.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Recommend approval as this tool is architecturally relevant and it is successfully implemented in the HeV infrastructure.

2.7) Advanced Billing Concept (ABC)

General Information

Website:	http://www.abccodes.com/ali/products_services/pro_description.asp
Description:	Advanced Billing Concept (ABC) Codes are five-digit Health Insurance Portability and Accountability Act (HIPAA) compliant alpha codes used by licensed and non-licensed healthcare practitioners on standard healthcare claim forms to describe services, remedies and/or supply items provided and/or used during patient visits.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	AAIHDS

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Current Procedural Terminology (CPT)

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2008	1/1/2008		
2009	1/1/2009		
2010	1/1/2010		

VA Forecast Information (10/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the

responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	**Please refer to the Windows Server entry for VA Forecast Information**

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.8) Advanced Encryption Standard (AES)

General Information

Website:	http://csrc.nist.gov/publications/PubsFIPS.html
Description:	FIPS 197: Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Vendor Name: NIST

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1	11/1/2001		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.9) Advanced Video Coding for Generic Audiovisual Services

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=H

Description: Advanced Video Coding for Generic Audiovisual Services is designed to enable the use of the coded video representation in a flexible manner for a wide variety of network environments. The use of this coding standard allows motion video to be manipulated as a form of computer data and to be stored on various storage media, transmitted and received over existing and future networks and distributed on existing and future broadcasting channels.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision FA

Source:	
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1	5/30/2003		
2	3/1/2005		
3	11/22/2007		
4	3/16/2009		
5	3/9/2010		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.10) AIX

General Information

Website: http://www-03.ibm.com/systems/p/os/aix/index.html

Description: Introduced in January of 1986, AIX is IBM's implementation of the UNIX operating system. AIX is derived from both AT&T Unix System V and 4.3 BSD and it offers the Korn (ksh) shell, Bourne (sh) and C (csh) shells. The current generation of this product, AIX 5L is open and conforms to The Open Group's Single UNIX Specification Version 3. It provides fully integrated support for 32- and 64-bit applications running concurrently in their full range of scalability. AIX 5L supports the IBM eServer p5, IBM eServer pSeries, IBM eServer i5 and IBM RS/6000 server product lines, as well as IntelliStation POWER and RS/6000 workstations. AIXL (AIX 5L) is IBM's key element to IBM's AIX / Linux affinity strategy, IBM is working to implement Linux API compatibility within AIX and deliver a common set of application development tools and utilities across AIX and Linux.

Decision: Approved

Decision Constraints: Products that have been deployed to a production environment may continue to use this technology. All other products must utilize a One-VA TRM approved Linux operating system.

Decision Source: ARB

Decision Process: TRM v2

Decision Date: 9/17/2008

Current Status: Analysis Completed

Introduced By: TRM Team

Vendor Name: IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	866: Dependent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Solaris
- Windows (Server)
- HP-UX
- Red Hat Linux

Companion Technologies/Standards:

- JDK - IBM Java Software Developer Kit related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
4.3	9/17/1999	6/30/2003	12/31/2003
5.3	8/4/2006	4/1/2011	4/1/2012
6.1	10/1/2007		

VA Forecast Information (04/09/2010)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
4.3	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
5.3	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
6.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Architectural Area

- Integration
- Data
- Application

Architectural Benefits

- Proprietary operating systems such as AIX are tightly coupled to the vendor's hardware enabling optimized operation, security and utilization of the enterprise's physical layer components.

Architectural Risks

- AIX is a proprietary system tightly coupled to proprietary hardware. Any need to replace the operating system at a later date could be complex, time consuming, and costly.

EA Requirement

- ENTR 68 (Inactive) - The entire suite of deployable software (i.e., Operating System, Database Engine, Mid-Tier, and Reports) shall be identified and documented.
- ENTR 91 - Deployment of new software and/or upgrades shall use standard tools and/or follow standard procedures established for use by the Office of Information.

Tier Used

- Data Tier
- Middle Tier (Infrastructure)

- Middle Tier (Business)
- Middle Tier (Integration)

Tool Type

- Platform

Tool Usage

- Development
- Runtime

General Assessment

Expected Usage:	The inclusion of AIX in the TRM fulfills the objectives outlined in ENTR68 and the management standardization objectives described in ENTR91 (note that both of these requirements are now marked as "inactive").
Assessment Type:	Refresh
Assessment Date:	9/15/2008
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	AIX is successfully implemented without issue.

2.11) ANT

General Information

Website:	http://ant.apache.org
Description:	ANother build Tool (ANT) is a Java-based build tool. ANT is similar to Make, but has greater cross platform compatibility. Make is extended with shell-based commands limited to the operating system; ANT is extended using Java classes-eliminating the need to write shell commands. ANT also uses XML-based configuration files that call out a target tree for executing various tasks in the Java compilation and build process.
Decision:	Approved

Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	ASF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	868: Software Configuration Management

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required for some configurations)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.6.0	12/18/2003		
1.6.1	2/14/2004		
1.6.2	7/16/2004		
1.6.3	4/28/2005		
1.6.4	5/19/2005		
1.6.5	6/2/2005		
1.7.0	12/19/2006		
1.7.1	6/27/2008		

VA Forecast Information (10/14/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.7.0	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
1.7.1	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment development and deployment of ANT is currently based on version 1.6.5.

General Analysis

Architectural Area

- Integration

Standards Traceability

- SGML (ISO 8879)

Tool Type

- Framework

Tool Usage

- Development

General Assessment

Expected Usage:	ANT provides a framework for scripting software builds, installation and configuration tasks.
Assessment Type:	Refresh
Assessment Date:	9/15/2008
Notes:	ANT is the leading framework automating build, configuration, installation and test execution. Although Maven is an alternative to ANT, they have different architectures; most projects will not be able to move from ANT to Maven without a major restructuring of the source code directory structure.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	ANT has been successfully implemented in the HeV infrastructure.

2.12) Apache Cactus

General Information

Website:	http://jakarta.apache.org/cactus/

Description:	Cactus, which is part of the Jakarta Project of Apache, is a unit testing framework for testing Java EE server-side code such as Enterprise Java Beans, Servlets, JSP, etc. Cactus differs from JUnit (JUnit is a Java unit testing framework), in that Cactus is specifically designed to aid in testing on the server.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	ASF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	869: Test Management

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JUnit - ***(required libraries)***
- Apache Commons - ***(required libraries)***
- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.4	8/25/2002		
1.4.1	8/31/2002		
1.5	11/23/2003		
1.6	5/8/2004		
1.6.1	5/14/2004		
1.7	1/28/2005		
1.7.2	3/26/2006		
1.8	4/11/2008		
1.8.1	1/26/2009		

VA Forecast Information (09/11/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009	CY2010	CY2011

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.6.1	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.7.2	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.8	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.8.1	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Architectural Area

- Application

Architectural Benefits

- Cactus provides a mechanism for automating and consistently implementing unit testing on the server (in the Java EE container); this improves code quality, portability, and interoperability.

Architectural Risks

- The deployment of Cactus may distract from the use of standardized tools from the Rational Tools suite; standardized technology is an attribute of architectural maturity.

Tier Used

- Middle Tier (Infrastructure)
- Middle Tier (Business)

Tool Type

- Framework

Tool Usage

- Development

General Assessment

Expected Usage:	A server-side Java EE unit testing framework.
Assessment Type:	Refresh
Assessment Date:	1/13/2009
Notes:	AspectJ is on the prohibited list in favor of Spring AOP aspect oriented programming. AspectJ is a compile and runtime dependency of Apache Cactus and the AspectJ library should only be used in support of Apache Cactus.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Approve with caution; alternatives from the Rational Tools suite should be exhausted before Cactus is deployed.

2.13) Apache Commons

General Information

Website:	http://commons.apache.org/
Description:	Formerly listed on the TRM as "Jakarta Commons Collections". Apache Commons is an open source project focused on all aspects of creating and maintaining a library of reusable Java components. One of the primary goals of the Apache Commons project is to ensure that the components have minimal dependencies on other libraries, to make deployments easier. Similarly, Commons components will keep their interfaces as stable as possible, so that end-users (including HeV projects) can implement these components without having to worry about future changes breaking deployed source code.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v3
Decision Date:	1/7/2009
Current Status:	Analysis Completed
Introduced By:	TRM Team

Vendor Name: ASF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Attributes	Runtime API to metadata attributes such as doclet tags.
BeanUtils	Easy-to-use wrappers around the Java reflection and introspection APIs
Betwixt	Services for mapping JavaBeans to XML documents, and vice versa
Chain	"Chain of Responsibility" pattern implementation
CLI	Command Line arguments parser
Codec	General encoding/decoding algorithms (for example phonetic, base64, URL)
Collections	Extends or augments the Java Collections Framework
Configuration	Reading of configuration/preferences files in various formats
Daemon	Alternative invocation mechanism for unix-daemon-like java code
DBCP	Database connection pooling services
DbUtils	JDBC helper library
Digester	XML-to-Java-object mapping utility
Discovery	Tools for locating resources by mapping service/reference names to resource names
EL	Interpreter for the Expression Language defined by the JSP 2.0 specification
Email	Library for sending e-mail from Java
Exec	API for dealing with external process execution and environment management in Java
FileUpload	File upload capability for your servlets and web applications
IO	Collection of I/O utilities
JCI	Java Compiler Interface
Jelly	XML based scripting and processing engine
Jexl	Expression language which extends the Expression Language of the JSTL

JXPath	Utilities for manipulating Java Beans using the XPath syntax
Lang	Provides extra functionality for classes in java.lang
Launcher	Cross platform Java application launcher
Logging	Wrapper around a variety of logging API implementations
Math	Lightweight, self-contained mathematics and statistics components
Modeler	Mechanisms to create Model MBeans compatible with JMX specification
Net	Collection of network utilities and protocol implementations
Pool	Generic object pooling component.
Primitives	Smaller, faster and easier to work with types supporting Java primitive types
Proxy	Library for creating dynamic proxies
SCXML	An implementation of the State Chart XML specification aimed at creating and maintaining a Java SCXML engine. It is capable of executing a state machine defined using a SCXML document, and abstracts out the environment interfaces.
Validator	Framework to define validators and validation rules in an xml file
VFS	Virtual File System component for treating files, FTP, SMB, ZIP and such like as a single logical file system

FEA Categories

Service Area	Service Category	Service Standard Code
N/A	N/A	N/A

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Quartz Enterprise Job Scheduler related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (11/16/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	The versioning information for each of the Apache Commons components vary by component. Consumers should target the latest version available for each component.

General Analysis

Architectural Area

- Application

Architectural Benefits

- Apache Commons promotes source code reuse which can enhace productivity and reduce software errors.

Architectural Risks

- None significant.

EA Requirement

- ENTR 1074 - Implement a One VA information technology framework that supports the integration of information across business lines and that provides a source of consistent, reliable, accurate, and secure information to veterans and their families, employees, and stakeholders (Enabling Objective E-3).

Tier Used

- Other Tier

Tool Type

- Open Source

Tool Usage

- Development

General Assessment

Expected Usage:	Reusabla Java source code components.
Assessment Type:	New
Assessment Date:	11/19/2008
Notes:	The Apache Commons project differs from many other Apache hosted projects because it is comprised of multiple, independently released packages. Each component in the Commons collection is versioned and released independently.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	The Apache Commons collection of Java API's promotes source code reuse and has a good track record in HeV (CISS has been using Commons under waiver 08-074).

2.14) Apache HTTP Server

General Information

Website:	http://www.apache.org/
Description:	Apache is an open-source HTTP (Web) server primarily used to serve both static content and dynamic Web pages for viewing in a Web browser.

Decision:	Approved
Decision Constraints:	To be used only on UNIX based platforms
Decision Source:	ARB
Decision Process:	TRM v3.2
Decision Date:	8/19/2009
Current Status:	Assessment Complete
Introduced By:	ARB
Vendor Name:	ASF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	871: Web Servers

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Internet Information Services (IIS)

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.3	6/5/1998		
2.0	4/6/2002		
2.2	12/4/2005		

VA Forecast Information (04/09/2010)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.3	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
2.0	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
2.2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Adoption Benefits

- Provides a low cost (open source) solution
- Mature product with very high market acceptance
- Well supported open source product

Adoption Risks

- Operational costs may be affected for having to support multiple web server technologies (training, monitoring, updates, etc.)

Architectural Benefits

- Platform independent - available on all VA approved operating systems

Standards Traceability

- HTTP
- SSL

Tier Used

- Presentation Tier (Web)
- Middle Tier (Infrastructure)

Tool Type

- Platform

Tool Usage

- Development
- Runtime

General Assessment

Expected Usage:	HTTP server for static and dynamic web pages
Assessment Type:	New
Assessment Date:	6/26/2009
Notes:	
Recommendation:	Approve
Recommendation Constraints:	To be used only on UNIX based platforms.
Recommendation Justification:	Apache HTTP is the world's most popular web server. It is extremely mature, has excellent market acceptance, and is well

supported.

2.15) Apache POI

General Information

Website: http://poi.apache.org/

Description: The Apache POI project is a set of APIs (Application Programming Interface) for reading-writing Microsoft Office file formats using pure Java.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: ARB

Decision Process: TRM v4

Decision Date: 9/16/2009

Current Status: Analysis Completed

Introduced By: TRM Team

Vendor Name: ASF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Business Logic	890: Platform Independent Technologies

Operating Systems Supported

- AIX

- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.0	6/1/2007		
3.1	6/30/2008		
3.2	10/19/2008		

VA Forecast Information (08/03/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009	CY2010	CY2011

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
3.2	None	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Adoption Benefits

- Apache POI offers Java code-level access to Microsoft file formats without licensing cost.

Adoption Risks

- None significant.

Architectural Benefits

- Apache POI is a vendor neutral API that facilitates access to common office file formats.

Architectural Risks

- None significant.

Standards Traceability

- ISO/IEC 29500:2008

General Assessment

Expected Usage:	The IT TRM team uses Apache POI to read from Excel spreadsheets with Java code.
Assessment Type:	New
Assessment Date:	8/3/2009
Notes:	The name "Apache POI" was originally an acronym for "Poor Obfuscation Implementation"; a witty reference to the fact that the Microsoft Office file formats were poorly obfuscated--as they have been reverse engineered successfully.
Recommendation:	Approve
Recommendation	Office 2007 Open XML file formats, such as XLSX and PPTX,

Constraints:	are not currently supported (but are planned for future releases).
Recommendation Justification:	The Apache POI APIs for Office 2003 file formats are stable, proven, open source and vendor neutral.

2.16) Apache Struts

General Information

Website:	http://struts.apache.org/
Description:	Apache Struts (formerly listed on the TRM as "Struts plus Tiles"), is a Java-based open source project sponsored by the Apache Software Foundation. The project is called “Struts” because the framework is meant to furnish the “invisible underpinnings” that support Web-based application development with Java. The Struts framework makes-up for the shortcomings of Java SE in thin-client and Web-based application development. Struts has evolved into two distinct versions: Struts 1 and Struts 2. Struts versions 1.x are mature, widely documented, implemented, (in HeV applications) and supported. Struts 2 is a completely new approach based on the merger of the WebWork framework and Struts.
Decision:	Approved
Decision Constraints:	• Projects deployed with Struts versions 1 should gradually migrate to the Spring framework as that transition is practicable. • New projects in technology planning should use the Spring framework instead of Struts. • Projects planning for the re-write of their applications to support Struts versions 2 should move to the Spring framework instead.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	ASF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	895: Middleware

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***
- Apache Commons - ***(required libraries)***

Comparable Technologies/Standards:

- Spring Framework

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.3.5	8/16/2006		
2.1.6	1/13/2009		
2.1.8	9/29/2009		
1.3.8	3/10/2007		
1.3.9	8/11/2007		
1.3.10	12/4/2008		
2.0.6	2/22/2007		
2.0.8	6/11/2007		
2.0.9	7/24/2007		
2.0.11	9/22/2007		
2.0.12	10/16/2008		

VA Forecast Information (10/14/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.3.5	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.3.8	Supported	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.3.9	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.3.10	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	**Version 2 of Struts is not approved for use.** The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment development and deployment of Struts is currently based on version 1.3.10.

General Analysis

Architectural Area

- Application

Architectural Benefits

- For projects already deployed on Struts, Struts 1 provides a reusable, standardized framework for producing Java applications using the Model View Controller design pattern.

Architectural Risks

- It appears that the Struts framework has reached the point where its innovation and adoption will begin to decline. Craig McClanahan, chief architect and author of Struts, has left the project for good--and he is urging current Struts users to migrate to newer Web frameworks.
- Struts is a Web (presentation) framework only; therefore by definition, the project will need to incorporate additional frameworks or Java-based helpers to complete an application. The use of multiple frameworks adds complexity and maintenance overhead.

Standards Traceability

- Java EE - EJB 3.0
- Java EE - JDBC 4.0

Tier Used

- Presentation Tier (Web)

Tool Type

- Framework

Tool Usage

- Development
- Management/Collaboration
- Runtime

General Assessment

Expected Usage: A Model View Controller based framework for developing

dynamic Web content with Java.

Assessment Type: Refresh

Assessment Date: 12/23/2008

Notes: Version 2 of the Apache Struts framework is a radical departure from version 1. Apache Struts 2 is in fact, the framework formerly known as WebWork. To change an application architecture from Struts 1 to Struts 2 will require a significant amount of rework time and resources. The advice of this analysis is to instead, use these resources to move to the Spring framework. The Spring framework contains all of the functionality found in Struts 1, as described here:

Struts Actions Are Spring Controllers
In Struts, Actions are core processing objects of the framework. They play the role of controllers in the MVC pattern. The Spring alternative to Struts Actions is the Controller interface. Spring Controllers process user input and dispatch to view components in Spring. The most significant differences between the Struts Action and the Spring Controller are that Actions are abstract classes and Controllers are interfaces. This design (also known as *design by interface*) minimizes the coupling between the application and the framework, and gives the architect greater flexibility in the design of the Controllers. With this in mind, the simplest intermediary transition step from Struts to Spring is to rewrite Actions so they implement the Controller interfaces and reuse the existing code. This allows incremental removal of all the Struts dependencies while keeping the application operational.
No Action Forms
One of the best things about the Spring framework is that it has no specialized ActionForm objects--Spring supports binding of HTTP form values directly into POJOs (Plain Old Java Objects). This feature greatly simplifies application maintenance by limiting the number of classes to create and maintain. A Struts ActionForm is not a true domain object--it is a place to hold user data until it can be validated and transferred into domain objects as commands. The advantage of the Struts ActionForm approach is that invalid data can be redisplayed easily; the disadvantage is that the data has to get into a domain object at some point, and Struts can only provide one-half of that solution. The Struts to Spring migration would mean dropping form beans and using domain objects directly--but this is not mandatory as it is still possible to use Form Bean objects as a map between the form inputs and domain objects.

ActionForwards versus ModelAndView
In Struts ActionMapping, objects are pointers into presentation resources (Actions, JSPs, Tiles, HTML files, etc.). The closest component in Spring MVC to ActionMapping is the ModelAndView interface. Spring Controllers return implementations of the ModelAndView interface, which like a Controller can be customized. Or, if appropriate, you can use the ModelAndView implementation supplied by Spring MVC. As the name implies, ModelAndView objects have Model and View components. Model components contain the business object to be displayed via the View component. Depending on the scenario, ModelAndView implementations may not have any Model components included. They may simply forward into some form of an actual View component (JSP, XSLT, Tiles, HTML, XML, etc.).

The migration from Struts 1 to Spring can be accomplished using one of the following strategies:

Strategy 1: Spring Enabling of Struts Components
For projects who want to migrate slowly, the first step is to enable Struts Actions as Spring Beans. This is a simple process, and the Spring documentation details it well. It does not require any changes to the existing Struts code, but it enables Struts Controller components, Actions, to be treated as Spring Beans. In this process, Actions inherit the nature of the Spring Beans and, therefore, start looking a lot like Spring Controllers.
Slow and step-wise migration is possible with this process. Each Action could be replaced one at a time by the Spring Controllers without rewriting the application at once and interrupting the existing page-flow sequences.

Strategy 2: Spring with Tiles
Another alternative, fully supported by the Spring framework, is to replace Struts Controllers and related components (Actions, Form Beans, etc.) with Spring MVC components while keeping Tiles as the pure “view” framework. Spring MVC does not have a specific alternative to Tiles, so architects may decide to keep their investments in Tiles and make them work through Spring MVC.
The one serious disadvantage of this approach is that you will effectively maintain two diverse Web frameworks in your Web application, which could result in a greater maintenance burden and training effort.

Strategy 3: Complete Migration
Complete migration would mean total replacement of all the components of the Struts framework with Struts MVC. At the end of the process, no Struts-specific components would remain in the application.

Recommendation: Approve-Conditional

Recommendation Constraints:

Recommendation Justification: The recommendation is to approve the continued use of Struts with conditions:

- Projects deployed with Struts versions 1 should gradually migrate to the Spring framework as that transition is practicable.
- New projects in technology planning should use the Spring framework instead of Struts.
- Projects planning for the re-write of their applications to support Struts versions 2 should move to the Spring framework instead.

Struts is a Web (presentation) framework only; therefore by definition, projects will need to incorporate additional frameworks or Java-based helpers to complete an application. The use of multiple frameworks adds complexity and maintenance overhead--so it is an architectural goal to reduce the number of frameworks used in the VA. In addition, Struts requires use of Struts-specific objects that couples the view (in the Model, View, Controller, or MVC pattern) to this particular technology. Another architectural goal is the separation of concerns so that any of the MVC elements can be changed without a major re-write of the application. Spring provides a MVC approach without any inherent dependencies to the framework.

2.17) Apache Tomcat

General Information

Website: http://tomcat.apache.org/

Description: Apache Tomcat is an open source software implementation of the Java Servlet and JavaServer Pages technologies. It provides a "pure Java" HTTP web server environment for Java code to run.

Decision:	Approved
Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	ASF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	871: Web Servers

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Hypertext Transfer Protocol (HTTP) related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5.5	8/31/2004		
6.0	12/1/2006		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
6.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.18) Application Oriented Sites

General Information

Description:	These services build on the Data-Oriented services by providing the ability to process complex logic (including transactions) based on a client's request.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Design Pattern	The implementation of these services should follow the Model-View-Controller (MVC) design pattern where the controller follows the servlet specification, the view follows the JSP or XSLT specification, and the model conforms to the JavaBean or POJO specification

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	887: Dynamic Server-Side Display

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.19) Architecture for IP Address Allocation with CIDR

General Information

Website:	http://tools.ietf.org/html/rfc1518
Description:	Architecture for IP Address Allocation with CIDR provides an architecture and a plan for allocating IP addresses in the Internet.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 1518	9/1/1993		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010	CY2011	CY2012

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 1518	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.20) Audit Services

General Information

Description: A system's audit trail is a collection of audit records containing data about security relevant events, i.e., attempted violations of the security policy and changes to the security state of the system. Audit services provide the meansto record the chronological set of related records that provide evidence of system activity.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Separation of Power		There shall be a separation of duties between security personnel who administer the access control function and those who administer the audit trail.

Training		Reviewers shall know what to look for to be effective in spotting unusual activity. They need to understand what normal activity looks like.
Audit Trail Reviews		• Develop guidelines that describe how frequently audit trails are reviewed and whether there arereview guidelines. • Application owners, data owners, system administrators, data processing function managers, andcomputer security managers should determine how much review of audit trail records is necessary, based on the importance of identifying unauthorized activities. • Design the system to allow audit trail function queries by user ID, terminal ID, application name,date and time, or some other set of parameters to run reports of selected information. This makes the Audit trail reviews easier and more efficient. • The appropriate system-level or application-level administrator should review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Audit Log Retention	Audit logs should be maintained for a retention period specified in the applicable security policy.
Audit Record	At a minimum, each audit record should include the following, if applicable: • The type of event • The date and time the event occurred • A success or failure indicator • The identity of the entity and/or operator that caused the event
Audit Actions	Actions taken as a result of these reviews should be documented.
ISO/IEC 10181-7	Security Audit and Alarms Framework
ISO/IEC 10164-8	Security Audit Trail Function

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.21) Basic Transition Mechanisms for IPv6 Hosts Routers

General Information

Website:	http://tools.ietf.org/html/rfc4213
Description:	Basic Transition Mechanisms for IPv6 Hosts Routers specifies IPv4 compatibility mechanisms that can be implemented by IPv6 hosts and routers. Two mechanisms are specified, dual stack and configured tunneling. Dual stack implies providing complete implementations of both versions of the Internet Protocol (IPv4 and IPv6), and configured tunneling provides a means to carry IPv6 packets over unmodified IPv4 routing infrastructures.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision	TRMSP 4.3.2

Process:
Decision Date: 3/14/2008
Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 4213	10/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 4213	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.22) Bing Maps

General Information

Website: http://www.microsoft.com/maps/developers/

Description: Microsoft's Bing Maps is composed of three APIs that VA developers can use to add mapping and location capabilities to applications.

The API's of Bing Maps include: Bing Map Control SDK, Bing Map Interactive SDK, and the Bing Web Services SDK.

Decision: Approved

Decision No constraints have been specified at this time.

Constraints:	
Decision Source:	ARB
Decision Process:	TRM v3.2
Decision Date:	8/19/2009
Current Status:	Analysis Complete
Introduced By:	Enterprise Tools Management
Vendor Name:	Microsoft

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	888: Content Rendering

Operating Systems Supported

- Red Hat Linux
- Windows (Client)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Google Maps

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
6.2	6/9/2009		

VA Forecast Information (06/18/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
6.2	None	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	The API's of Bing Maps include: Bing Map Control SDK, Bing Map Interactive SDK, and the Bing Web Services SDK. The forecast references the Bing Map Control SDK as the versioning of the client-side control will be the primary driver in the suite of APIs.

General Analysis

Adoption Benefits

- An alternative to Google Maps.

Adoption Risks

- None significant.

Architectural Benefits

- Thin client presentation of Bing Maps is consistent with the HEV paradigm.

Architectural Risks

- None significant.

Standards Traceability

- AJAX

Tier Used

- Presentation

General Assessment

Expected Usage:	Embed maps in applications where location data is required.
Assessment Type:	New
Assessment Date:	6/18/2009
Notes:	Bing Maps is not 508 compliant. However, an alternative can be presented. For example, offering a map view but also a "list view" that does not use JavaScript and is screen reader friendly.
Recommendation:	Approve
Recommendation Constraints:	Section 508 issues must be addressed by the implementer.
Recommendation Justification:	Bing Maps provides an alternative to Google Maps with some user interface advantages. Bing Maps is standards-based (AJAX) and is platform independent.

2.23) Biometric Application Programming Interface (BioAPI)

General Information

Website:	http://www.iso.org/iso/catalogue_detail.htm?csnumber=33922
Description:	ISO/IEC 19784 (formerly ANSI INCITS 358): Biometric Application Programming Interface (BioAPI) provides a defined interface that allows a software application to communicate with (utilize the services of) one or more biometric technologies. It includes a high-level generic biometric authentication model suited to a broad range of biometrically enabled applications and to most forms of biometric technology. An architectural model is described which enables components of a biometric system to be provided by different vendors, and to interwork through fully-defined Application Programming Interfaces (APIs), corresponding Service Provider

Interfaces (SPIs), and associated data structures. BioAPI covers the basic biometric functions of enrollment, verification and identification, and includes a database interface to allow an application to manage the storage of biometric records.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
BioAPI specification	This document defines the interface that allows a software application to communicate with (utilize the services of) one or more biometric technologies.
Biometric archive function provider interface	This document defines the interface between a biometric service provider (BSP) and a biometric archive function provider (BAFP) for BioAPI.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	3/1/2000		
1.1 (ANSI/INCITS 358)	1/1/2002		
2.0 (ISO/IEC 19784)	1/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.1 (ANSI/I	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

NCITS 358)												
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.24) Biometric Information Management and Security

General Information

Website: http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+X9.84%3a2003

Description: Biometric Information Management and Security for the Financial Services Industry specifies the minimum security requirements for effective management of biometric data. Within the scope of this Standard the following topics are addressed: Security for the collection, distribution, and processing, of biometric data, encompassing data integrity, authenticity, and non-repudiation; Management of biometric data across its life cycle comprised of the enrollment, transmission and storage, verification, identification, and termination processes; Usage of biometric technology, including one-to-one and one-to-many matching, for the identification and authentication of banking customers and employees; Application of biometric technology for internal and external, as well as logical and physical access control; Encapsulation of biometric data; Techniques for the secure transmission and storage of biometric data; Security of the physical hardware used throughout the biometric data life cycle; Techniques for integrity and privacy protection of biometric data.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: ANSI

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2003	1/1/2003		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2003	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.25) Biometric Services

General Information

Description: Biometrics deals with the automated methods of authenticating or verifying an individual based upon a physical or behavioral characteristic.<br
Biometrics is the science and technology of measuring and statistically analyzing biological data. Biometrics usually refers to technologies for measuring and analyzing human body characteristics such as fingerprints, eyeretinas and irises, voice patterns, facial patterns, and hand measurements, especially for authentication purposes.

Fingerprint and other biometric devices consist of a reader or scanning device, software that converts the scannedinformation into digital form, and wherever the data is to be analyzed, a database that stores the biometric data for comparison with previous records. When converting the biometric input, the software identifies specific points of data as match points. The match points are processed using an algorithm into a value that can be compared with biometric data scanned when a user tries to gain access.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
NIST FIPS 48	Guidelines On Evaluation Of Techniques For Automated Personal Identification
NIST FIPS 190	Guideline For The Use Of Advanced Authentication Technology Alternatives
CDSA/CSSM Authentication: HRS API	Common Data Security Architecture (CDSA)/Common Security Services Manager (CSSM) Authentication: Human Recognition Service (HRS) API
ISO/IEC 7816-11	Personal Verification Through Biometric Methods

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.26) BIRT

General Information

Website:	http://www.eclipse.org/birt/phoenix/
Description:	Business Intelligence and Reporting Tools (BIRT) is an open-source eclipse based project that provides reporting capabilities, specifically for web and client applications based on Java. BIRT has two main components: a runtime component that can be deployed into a Java EE container and an Eclipse based report designer. The BIRT project also includes a charting engine that is integrated into the report designer or can be used as a standalone component. BIRT can be used to produce reports in several different formats including HTML, PDF, PPT, and postscript formats. BIRT has APIs for design, report and chart engines and includes database drivers for several different data sources.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v3.2

Decision Date: 8/19/2009
Current Status: Analysis Completed
Introduced By: Enterprise Tools Management
Vendor Name: Eclipse

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Management	894: Reporting and Analysis

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Eclipse - ***(required libraries)***
- iText Core - ***(required libraries)***
- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	6/6/2005		
2.0	1/22/2006		
2.1	7/1/2006		
2.2	6/29/2007		
2.3	6/25/2008		
2.5	6/24/2009		
2.6 (est)	5/31/2010		

VA Forecast Information (06/25/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2.2	None	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
2.3	None	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
2.5	None	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Adoption Benefits

- None significant.

Adoption Risks

- None significant.

Architectural Benefits

- None significant.

Architectural Risks

- None significant.

Tier Used

- Presentation Tier (Web)
- Client Tier
- Middle Tier (Infrastructure)

Tool Type

- Tool
- Framework

Tool Usage

- Development
- Runtime
- Management/Collaboration

General Assessment

Expected Usage:	Enterprise Exception Logging Service (EELS)
Assessment Type:	New
Assessment Date:	6/26/2009
Notes:	The BIRT Report Designer Framework has dependencies on the following Eclipse projects: Eclipse, DTP, EMF, GEF, and WTP. BIRT also depends on Java as well. For specific version information on dependences, check the BIRT download/installation instructions for the specific release of BIRT.
Recommendation:	Approve

Recommendation Constraints:	
Recommendation Justification:	BIRT is a top level project within the Eclipse Foundation with consistent releases being offered and has been adopted by many organizations including IBM Tivoli for common reporting within that toolset. The scope of this assessment includes the runtime reporting engine and the Eclipse based report designer.

2.27) BlazeDS

General Information

Website:	http://opensource.adobe.com/wiki/display/blazeds/BlazeDS
Description:	BlazeDS is Adobe's open source server-based middleware component, providing messaging between back-end applications. BlazeDS provides a publish/subscribe infrastructure for real-time messaging.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v4.1
Decision Date:	10/28/2009
Current Status:	Analysis Completed
Introduced By:	ARB
Vendor Name:	Adobe

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	895: Middleware

Operating Systems Supported

- Red Hat Linux
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***
- Flex SDK - ***(required for some configurations)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.0	2/14/2008		
3.0.1	5/15/2008		
3.2	11/1/2008		
3.3 (est)			

VA Forecast Information (10/08/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on

the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
3.2	None	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
3.3 (est)	None	None	None	None	None	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Adoption Benefits

- Binary data transfer between client and server is much faster than other than text based transports like SOAP or XML.

Adoption Risks

- None significant.

Architectural Benefits

- BlazeDS provides an open adapter architecture making for easier integration with other data sources.
- BlazeDS provides server side adapters that clients to dynamically acquire configuration needs at connect time.

Architectural Risks

- BlazeDS has a proprietary binary data encoding protocol, Action Message Format (AMF) for data transmission and remote method invocation. While Adobe has released the specification and source code for AMF and BlazeDS, the potential for protocol lock-in is present.

Tool Type

- Messaging middleware.

General Assessment

Expected Usage:	BlazeDS provides data services between server side java and Flex internet applications.
Assessment Type:	New
Assessment Date:	10/9/2009
Notes:	Support for BlazeDS is provided, at cost, through the LiveCycle Data Services ES2 support program. BlazeDS was originally a component within the Adobe LiveCycle Enterprise Suite and was contributed as an open source offering in December, 2007 . BlazeDS 3.2 requires JDK 1.5 or higher.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	BlazeDS is an open source technology developed and supported by Adobe. It is a mature codebase and is currently in use in production in the VA as a messaging middleware component.

2.28) BMC Mainview

General Information

Website:	http://www.bmc.com/products/brand/mainview.html
Description:	BMC Mainview provides historical performance monitoring in a single mainframe solution that integrates across z/OS, z/VM, Linux, and subsystems.
Decision:	Approved
Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components

Vendor Name: BMC Software

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	Network Management Services*

Operating Systems Supported

- Red Hat Linux
- z/OS
- z/VM

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- BMC Performance Manager
- Wily Introscope
- Strobe

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2.8			
2.9	8/1/2008		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2.8	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.29) BMC Performance Manager

General Information

Website: http://www.bmc.com/patrol/

Description: BMC Performance Manager, formerly knowna as BMC Patrol, is a systems management and optimization suite for computing infrastructure that provides automated problem resolution, performance analysis and optimization.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	BMC Software

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
N/A	N/A	N/A

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Wily Introscope
- Foglight

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Architectural Area

- Application
- Data
- Integration

Architectural Benefits

- BMC is focused on the availability and performance of computing assets in the operational environment.

Architectural Risks

- None Significant

Tier Used

- Data Tier

- Presentation Tier
- Client Tier
- Infrastructure Tier
- Business Logic Tier
- Integration Tier

Tool Type

- Commercial

Tool Usage

- Runtime - Embedded
- Development
- Runtime

General Assessment

Expected Usage: Performance Manager provides the ability to proactively monitor operating systems, applications, databases, and networks.

Assessment Type: Refresh

Assessment Date: 2/13/2009

Notes: BMC Patrol products are individually and uniquely versioned. As such, there is no benefit to providing a forecast since it would reflect only a single BMC Patrol component.

At a minimum, the VA has the following BMC components deployed:

- BMC Performance Manager Central Console is version 7.5.00
- BMC Performance Manager Agent is version 7.3.30
- BMC Performance Manager for BEA WebLogic is version 2.6.10
- BMC Performance Manager for Internet Servers is version 6.2.50
- BMC Performance Manger for DataBases is version 2.6.00
- BMC Performance Assurance is version 7.4.10

Recommendation: Approve

Recommendation Constraints:

Recommendation Justification:	VA Operations currently uses Microsoft Operations Manager for systems availability monitoring. However, Microsoft Operations Manager currently does not support Linux clients. Recommend approval since Linux is already an existing standard.

2.30) Bobby

General Information

Website:	http://www.watchfire.com/products/webxm/bobby.aspx
Description:	Watchfire Bobby is a web accessibility desktop testing tool designed to help expose barriers to accessibility and encourage compliance with existing accessibility guidelines, including Section 508 of the US Rehabilitation Act and the W3C's Web Content Accessibility Guidelines (WCAG). Bobby spiders through a website and tests on a page-by-page basis to see if it meets several accessibility requirements, including readability by screen readers, the provision of text equivalents for all images, animated elements, and audio and video displays. Bobby can see local web pages, as well as web pages behind your firewall. It performs more than 90 accessibility checks. During a scan, Bobby checks HTML against select accessibility guidelines and then reports on the accessibility of each web page. This tool is used extensively in HeV for 508 compliance.
Decision:	Approved
Decision Constraints:	NOTE: As of February 1, 2008 the Watchfire WebXact and Bobby Online products will no longer be publicly available. As an IBM Company, Watchfire will continue to invest in accessibility through the IBM Rational Policy Tester Accessibility Edition solution (previously WebXM Accessibility Module).
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	Watchfire

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	869: Test Management

Operating Systems Supported

- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Internet Explorer - ***(required for some configurations)***
- Firefox - ***(required for some configurations)***

Comparable Technologies/Standards:

- Rational Policy Tester

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5.0	6/1/2007		

VA Forecast Information (10/01/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
5.0	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
Forecast Note:												

General Analysis

Architectural Area

- Application

Architectural Benefits

- Architecturally, 508 compliance is a key objective which has been established for all interactive HeV capabilities. The need to make HeV both available and accessible to disabled users directly serves the HeV user community.

Architectural Risks

- None

EA Requirement

- ENTR 296 - Specifically supports Section 508 compliance objectives.
- ENTR 242 - Restore the capability of veterans with disabilities to the greatest extent possible and improve the quality of their lives and that of their families.

Tier Used

- Presentation Tier (Thick)
- Presentation Tier (Web)
- Client Tier

Tool Type

- Tool

Tool Usage

- Development
- Runtime

General Assessment

Expected Usage:	The use of assistive technology assessment tools such as Bobby directly facilitates compliance with 508 objectives set forth in ENTR 242 and 296. These enterprise requirements are dictated by legislative mandates as well as VA and VHA policy.
Assessment Type:	Refresh
Assessment Date:	2/12/2009
Notes:	Depends on Windows XP SP1 or Windows Server 2003 and Internet Explorer 5.5 SP2 or 6. IBM acquired Watchfire in July of 2007. As of 2/1/2008, Watchfire products are no longer publicly available. IBM now offers an accessibility testing solution called IBM Rational Policy Tester Accessibility Edition, which will be available as a licensed tool for HeV once support for IBM Rational Policy Tester Accessibility Edition is added to the contract.
Recommendation:	Approve
Recommendation Constraints:	NOTE: As of February 1, 2008 the Watchfire WebXact and Bobby Online products will no longer be publicly available. As an IBM Company, Watchfire will continue to invest in accessibility through the IBM Rational Policy Tester Accessibility Edition solution (previously WebXM Accessibility Module).
Recommendation Justification:	Recommend approval as this tool is architecturally relevant to the stated requirements, and it is currently successfully implemented in the HeV and VistA infrastructures.

2.31) Border Gateway Protocol (BGP)

General Information

Website:	http://tools.ietf.org/html/rfc4271
Description:	Border Gateway Protocol (BGP) defines an inter-autonomous

system routing protocol for the Internet.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 1771	3/1/1995		
RFC 4271	1/1/2006		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 4271	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.32) Broadband Audiovisual Communication Systems and Terminals

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=H

Description: ITU-T H.310: Broadband Audiovisual Communication Systems and Terminals covers the technical requirements for the systems and terminals of broadband audiovisual communication services defined in H.200/AV.100-series Recommendations. Both H.310 unidirectional and bidirectional broadband audiovisual terminals are defined. The classification of H.310 terminals into different terminal types is based on a set of audiovisual, network adaptation, and signalling capabilities. With these capabilities, H.310 terminals support a wide range of conversational and distributive applications and services. This revision enhances the interworking between different type of H.310 terminals.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2	9/25/1998		
2.1	1/8/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.33) BusinessWare

General Information

Website:	http://www.vitria.com/BusinessWare
Description:	BusinessWare is Vitria's platform for integrating complex transaction and process-based applications. Vitria combines broad capabilities for application integration with Business Process Management (BPM) and Business-to-Business (B2B) integration, providing a unified solution for modeling, implementing, monitoring, and managing end-to-end processes that span multiple systems and organizations.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	Vitria

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	896: Enterprise Application Integration

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Mirth Connect
- eGate Integrator

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.1.7			
4.3			

VA Forecast Information (10/14/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on

the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
3.1.7	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
4.3	Evaluation	Evaluation	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Architectural Area

- Integration
- Data

Architectural Benefits

- BusinessWare offers common infrastructure toolsets and middleware which support standardized developer skill sets and the implementation of best practices. The ability to provide opportunities for inter application connectivity and interaction contribute to the architectural goals of a modular component based HeV.

Architectural Risks

- Stability - Product deployment and operational stability are significant risks. Vitria, as it has been implemented in HeV, has been prone to deployment complexity, stability and operational issues that have impacted other applications in the HeV enterprise.

EA Requirement

- ENTR 586 (Inactive) - The Vitria BusinessWare Interface Engine shall be the preferred integration mechanism when designated message routing and destination management is required.

Standards Traceability

- SOAP
- EJB
- WSDL
- JMS
- JAX
- JMX
- UDDI
- AS2
- ebXML

Tier Used

- Middle Tier (Infrastructure)
- Middle Tier (Integration)
- Middle Tier (Business)
- Data Tier
- Client Tier

Tool Usage

- Runtime
- Development

General Assessment

Expected Usage:	Middleware components like Vitria provide key generalized capabilities, which are used throughout the enterprise. Such components provide major efficiencies to the development of individual applications by providing enterprise-level common components.
Assessment Type:	Refresh
Assessment Date:	2/2/2009
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Recommend approval as Vitria is successfully implemented in the HeV infrastructure.

2.34) Cache Database Engine

General Information

Website: http://www.intersystems.com/cache/index.html

Description: Cache identifies itself as a post-relational database, providing a high performance data repository with object driven features. It provides a multi-dimensional data engine where data is stored in sparse multi-dimensional arrays. It offers high performance with scalability and space efficient data storage. Data can be modeled as objects supporting encapsulation, multiple inheritance, polymorphism, embedded objects, references, collections, relationships, Binary Large Objects (BLOBs), as well as traditional SQL based relational data access. Java support is provided through both object-relational mapping and use of JDBC (Type 4) drivers. Cache classes can be projected as a Java class so properties and methods can be accessed as Enterprise Java Beans (EJB) or POJO (Plain Old Java Object) class descriptions.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: ARB

Decision Process: TRM v2

Decision Date: 9/17/2008

Current Status: Analysis Completed

Introduced By: Extended Tool List (ETL)

Vendor Name: InterSystems

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Database/Storage	875: Database

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)
- OpenVMS

Technologies/Standards Relationships

Runtime Dependencies:

- Structured Query Language (SQL) - ***(required for some configurations)***
- Extensible Markup Language (XML) - ***(required for some configurations)***

Comparable Technologies/Standards:

- Oracle Database
- SQL Server

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5.0	7/17/2003		
5.1	12/9/2005		
5.2	6/15/2006		
5.2.3	9/1/2006		
2007.1	6/4/2007		
2008.1	1/30/2008		
2008.2	10/10/2008		
2009.1	6/30/2009		

2010.1 (est)	2/1/2010		

VA Forecast Information (09/11/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
5.2.3	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
2007.1	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
2008.1	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
2009.1	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
2010.1 (est)	None	None	None	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Architectural Area

- Data

Architectural Benefits

- The data repository is a critical infrastructure component which underlies both the HeV and legacy VistA architectures. It directly facilitates application performance, scalability and capability; as well as the integrity and availability of data throughout the enterprise.

Architectural Risks

- Excessive complexity, vendor lock-in. Caché is currently deployed with Oracle as enterprise repositories in HeV. This diversity significantly complicates COOP, monitoring, interoperability, tuning, optimization, and capacity planning.

EA Requirement

- ENTR 62 (Inactive) - Applications which require VistA Legacy interface shall identify whether current VMS/Cache or future Linux/Cache/SQL databases is required.
- ENTR 68 (Inactive) - The entire suite of deployable software (i.e., Operating System, Database Engine, Mid-Tier, and Reports) shall be identified and documented.

Tier Used

- Middle Tier (Infrastructure)
- Data Tier

Tool Type

- Platform

Tool Usage

- Runtime

General Assessment

Expected Usage:	For HeV projects, Caché fulfills a need for a fast, object-oriented approach to data storage and retrieval.
Assessment Type:	Refresh
Assessment Date:	9/9/2008
Notes:	The Caché database is approved for use for small HeV projects. Note that vendor lock-in can occur with proprietary access mechanisms (such as Caché Objects); therefore, only ODBC or JDBC should be used with Caché.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Caché has been successfully implemented in the HeV infrastructure.

2.35) Cache JDBC Driver

General Information

Website: http://vista.intersystems.com/csp/docbook/DocBook.UI.Page.cls?KEY=TJAV_JDBCBackground

Description: Caché JDBC Driver is a high-performance Level 4 JDBC database driver. It is pure Java and involves no Caché-specific binary code and no JDBC-ODBC bridge. The Caché JDBC Driver supports the JDBC 2.0 API.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: HSD&D

Decision Process: ETL

Decision Date: 12/1/2006

Current Status: Introduced

Introduced By: Extended Tool List (ETL)

Vendor Name: InterSystems

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Management	893: Database Connectivity

Operating Systems Supported

- AIX

- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)
- OpenVMS

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Oracle JDBC Drivers

Companion Technologies/Standards:

- Java SE related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (09/11/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

ETL Approved Technology/Standard, TRM Analysis still pending.

General Assessment

ETL Approved Technology/Standard, TRM Assessment still pending.

2.36) Call Signalling Protocols and Media Stream Packetization

General Information

Website:	http://www.itu.int/itu-t/recommendations/index.aspx?ser=H
Description:	ITU-T H.225: Call signalling protocols and media stream packetization for packet-based multimedia communication systems covers the technical requirements for narrow-band visual telephone services defined in ITU-T H.200 and F.720-series Recommendations, in those situations where the transmission path includes one or more packet-based networks, each of which is configured and managed to provide a non-guaranteed Quality of Service (QoS) which is not equivalent to that of N-ISDN, such that additional protection or recovery mechanisms beyond those mandated by ITU-T Rec. H.320 need be provided in the terminals. It is noted that ITU-T Rec. H.322 addresses the use of some other LANs which are able to provide the underlying performance not assumed by the ITU-T Recs H.323 and H.225.0.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5	7/14/2003		
6	5/29/2005		

6.1	1/13/2007		
7	12/14/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
6	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.37) Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

General Information

Website: http://standards.ieee.org/getieee802/802.3.html

Description: IEEE 802.3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications - Ethernet local area network operation is specified for selected speeds of operation from 1 Mb/s to 10 Gb/s using a common media access control (MAC) specification and management information base (MIB). The Carrier Sense Multiple Access with Collision Detection (CSMA/CD) MAC protocol specifies shared medium (half duplex) operation, as well as full duplex operation. Speed specific Media Independent Interfaces (MIIs) allow use of selected Physical

Layer devices (PHY) for operation over coaxial, twisted pair or fiber optic cables. System considerations for multisegment shared access networks describe the use of Repeaters which are defined for operational speeds up to 1000 Mb/s. Local Area Network (LAN) operation is supported at all speeds. This specification includes:

- 100 Mb/s baseband network, type 100BASE-T
- 1000 Mb/s baseband network
- 10Gb/s baseband network
- Ethernet for subscriber access networks

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IEEE

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	Campus Area Network (CAN)*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2005	1/1/2005		
2008	1/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2005	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.38) Cascading Style Sheets (CSS)

General Information

Website:	http://www.w3.org/TR/CSS2/
Description:	Cascading Style Sheets (CSS) is a style sheet language that allows authors and users to attach style (e.g., fonts and spacing) to structured documents (e.g., HTML documents and XML applications). By separating the presentation style of documents from the content of documents, CSS simplifies Web authoring and site maintenance.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	888: Content Rendering

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2	5/12/1998		
2.1	9/8/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo

	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted
2.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.39) Cascading Style Sheets Mobile Profile (CSS-Mobile)

General Information

Website: http://www.w3.org/TR/css-mobile/

Description: This specification defines in general a subset of CSS that is to be considered a baseline for interoperability between implementations of CSS on constrained devices (e.g. mobile phones). Its intent is not to produce a profile of CSS incompatible with the complete specification, but rather to ensure that implementations that due to platform limitations cannot support the entire specification implement a common subset that is interoperable not only amongst constrained implementations but also with complete ones.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	888: Content Rendering
Service Platform and Infrastructure	Support Platform	864: Wireless / Mobile

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Cascading Style Sheets (CSS) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2.0	12/10/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.40) Castor XML

General Information

Website: http://www.castor.org/

Description: XML data binding framework to bind XML artifacts to Java objects and vice versa.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: HSD&D

Decision Process: ETL

Decision Date: 12/1/2006

Current Status: Introduced

Introduced By: Extended Tool List (ETL)

Vendor Name: Castor

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- JAXB Reference Implementation

Companion Technologies/Standards:

- Xerces related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.1.2	6/17/2007		
1.2	2/4/2008		

VA Forecast Information (09/11/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.1.2	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

ETL Approved Technology/Standard, TRM Analysis still pending.

General Assessment

ETL Approved Technology/Standard, TRM Assessment still pending.

2.41) Checksum Hash Value

General Information

Description: A checksum or hash value is used to detect errors or manipulation during transmission.

A checksum is a count of the number of bits in a transmission unit that is included with the unit so that the receivercan check to see whether the same number of bits arrived. If the counts match, it's assumed that the complete transmission was received. Both TCP and UDP communication layers provide a checksum count and verification as one of their services.

Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. The hashing algorithm is called the hash function. A good hash function should not produce the same hash value from two different inputs. In this manner, comparison of hash values can be used to verify the integrity of a data file or element.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
NIST FIPS 113	Computer Data Authentication
NIST SP 500-156	Message Authentication Code (MAC) Validation System: Requirements and Procedures
NIST SP 800-21	Guideline for Implementing Cryptography in the Federal Government
NIST SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
NSA - Network Security Guide	The 60 Minute Network Security Guide

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.42) Classless Inter-Domain Routing (CIDR)

General Information

Website:	http://tools.ietf.org/html/rfc4632
Description:	Classless Inter-Domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan discusses the strategy for address assignment of the existing 32-bit IPv4 address space with a view toward conserving the address space and limiting the growth rate of global routing state.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 1519	9/1/1993		
RFC 4632	8/1/2006		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or

production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 4632	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.43) Coding of Speech Using Low-Delay Code Excited Linear Prediction

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=G

Description: ITU-T G.728: Coding of Speech at 16 kbit/s Using Low-Delay Code Excited Linear Prediction contains the description of an algorithm for the coding of speech signals at 16 kbit/s using low-delay code excited linear prediction (LD-CELP).

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.8	2/17/2000		
1.9	5/29/2006		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.9	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.44) Common Biometric Exchange Formats Framework (CBEFF)

General Information

Website: http://csrc.nist.gov/publications/PubsNISTIRs.html

Description: NIST IR 6529 A: Common Biometric Exchange formats Framework (CBEFF) describes a set of data elements necessary to support biometric technologies in a common way. These data elements can be placed in a single file used to exchange biometric information between different system components or between systems. The result promotes interoperability of biometric-based application programs and systems developed by different vendors by allowing biometric data interchange.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	NIST

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
6529-A	4/5/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.45) Common Language Infrastructure (CLI)

General Information

Website: http://www.ecma-international.org/publications/standards/Ecma-335.htm

Description: ISO/IEC 23271 & ECMA-332: This standard defines the Common Language Infrastructure (CLI) in which applications written in multiple high-level languages can be executed in different system environments without the need to rewrite those applications to take into consideration the unique characteristics of those environments.

Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ECMA

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Technical Report on Information Derived from Partition IV XML File	

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
4	6/1/2010		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
4	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.46) Common Object Request Broker Architecture (CORBA)

General Information

Website:	http://www.omg.org/technology/documents/corba_spec_catalog.htm
Description:	Common Object Request Broker Architecture (CORBA) is a vendor-independent architecture and infrastructure that computer applications use to work together over networks. Using the standard protocol IIOP, a CORBA-based program from any vendor, on almost any computer, operating system, programming language, and network, can interoperate with a CORBA-based program from the same or another vendor, on almost any other computer, operating system, programming language, and network.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	OASIS

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Interfaces	This document specifies the CORBA Object Model and uses concepts from that model to define the operation of the Object Request Broker (ORB). The ORB is the basic mechanism by which objects transparently make requests to - and receive responses from - each other on the same machine or across a network.
Interoperability	This document specifies a comprehensive, flexible approach to supporting networks of objects that are distributed across and managed by multiple, heterogeneous CORBA-compliant Object Request Brokers (ORBs).

Components	This specification defines: • The syntax and semantics of a component model • A language to describe the structure and state of component implementations • A programming model for constructing component implementations • A runtime environment for component implementations • Interaction between components and Enterprise Java Beans • Meta-data for describing component-based applications, and interfaces for their deployment • A lightweight subset of the component model, programming model and runtime environment

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	895: Middleware

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.0	6/2/2001		
3.1	4/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
3.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.47) Common Warehouse Metamodel (CWM)

General Information

Website: http://www.omg.org/technology/documents/modeling_spec_catalog.htm

Description: The Common Warehouse Metamodel (CWM) defines interfaces that can be used to enable easy interchange of warehouse and business intelligence metadata between warehouse tools, warehouse platforms and warehouse metadata repositories in distributed heterogeneous environments.

Decision: Approved

Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	OMG

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Database/Storage	Warehouse Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.1	3/2/2003		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.48) Computer Based Training Exchange

General Information

Description: Computer Based Training (CBT) Exchange standards support the development, deployment, and interoperability of CBT and Learning systems.

Decision: Approved

Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
AICC AGR006 - Computer Managed Instruction (CMI)	This document recommends guidelines that promote the interoperability of CMI systems.
AICC AGR010 - Web-based Computer Managed Instruction (CMI)	This document recommends guidelines that promote the interoperability of Web-Based CMI systems.
AICC CMI001 - AICC/CMI Guidelines For Interoperability	This document defines the following: • The mechanism used by the CMI to launch CBT content • Common mechanisms and data for CMI/CBT communication • A common definition for organization and sequencing of CBT content in a course

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.49) Computer Graphics Metafile (CGM)

General Information

Website:	http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
Description:	The Computer Graphics Metafile provides a file format suitable for the storage and retrieval of picture information. The file format consists of a set of elements that can be used to describe pictures in a way that is compatible between systems of different architectures and devices of differing capabilities and design. This picture description includes the capability for describing static pictures. Static pictures are those where elements which may lead to dynamic effects (for example those leading to regeneration) are prohibited within the picture body.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Functional specification	
Binary encoding	

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	888: Content Rendering

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1999	12/15/1999		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1999	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.50) Confidentiality Framework

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=24329

Description: ISO/IEC 10181-5: The Information technology - Open Systems Interconnection - Security frameworks for open systems: Confidentiality framework specifies a general framework for the provision of confidentiality services.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1996	1/1/1996		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1996	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.51) Confidentiality Services

General Information

Description: Confidentiality refers to keeping electronic data private; i.e., preventing unauthorized individuals or processes fromgaining access to documents, transactions, data, or messages. Confidentiality services ensure that data is notmade available or disclosed to unauthorized individuals or computer processes. This is

accomplished through theuse of data encryption, security association, and key management. In addition, these services ensure thatobservation of usage patterns of communications resources is not possible.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Scope		Confidentiality services shall be applied to devices that permit human interaction with the information system.
SSL		Servers that use SSL shall be configured to enable SSL only.
Certification		All software and hardware providing encryption services shall be certified according to the FIPS 140 - Security Requirements for Cryptographic Modules standards.
Data Storage Encryption Algorithm		Data at rest encryption shall employ products that use the symmetric data encryption algorithm AES

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
E-mail Encryption	E-mail encryption should be deployed as S/MIME based solutions. PKI supports trusted digital signatures in S/MIME messages and should be utilized to implement e-mail encryption.
ISO/IEC 10181-4	Non-repudiation Framework

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	885: Supporting Security Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.52) Configuration Management

General Information

Description: Configuration management is the management of system change. Configuration management includes procedures for change control, system and network building, network baselining, auditing, and version management. Configuration management establishes change control. The challenge of change is that a change to the network is likely to introduce new faults or expose other faults that had not been observed prior to the change. Change control procedures ensure that the changes to a system are made in a controlled way so that their effect on the system can be predicted. Version management refers to keeping track of the version of operating systems running on the network devices.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Network Management		The network management system shall display management data, monitor and control managed devices, and communicate with management agents. Data link and physical layer parameters shall be monitored by management systems that are based on Management Information Base (MIB) - Remote Monitoring (RMON) standards.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Configuation Management Database	A configuration management database should be used to house information about network configurations. When a network is operational, it is important that changes be implemented using a controlled methodology.
Management Device	A router, server, switch, or end system should be selected on each network to be a local management device.
Configuration Management	After a configuration is verified and validated, it should be stored for future reference

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	Network Management Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.53) Control Protocol for Multimedia Communication

General Information

Website:	http://www.itu.int/itu-t/recommendations/index.aspx?ser=H
Description:	ITU-T H.245: Control Protocol for Multimedia Communication specifies syntax and semantics of terminal information messages as well as procedures to use them for in-band negotiation at the start of or during communication. The messages cover receiving and transmitting capabilities as well as mode preference from the receiving end, logical channel signalling, and Control & Indication. Acknowledged signalling procedures are specified to ensure reliable audiovisual and data communication.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
12	10/7/2005		
13	5/29/2006		
14	6/13/2008		
15	12/14/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
13	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.54) Cryptographic Algorithm Implementation Requirements for ESP and AH

General Information

Website: http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

Description: The IPsec series of protocols makes use of various cryptographic algorithms in order to provide security services. The Encapsulating Security Payload (ESP) and the Authentication Header (AH) provide two mechanisms for protecting data being sent over an IPsec Security Association (SA). To ensure interoperability between disparate implementations, it is necessary to specify a set of mandatory-to-implement algorithms to ensure that there is at least one algorithm that all implementations will have available. Cryptographic Algorithm Implementation Requirements for ESP and AH defines the current set of mandatory-to-implement algorithms for ESP and AH as well as specifying algorithms that should be implemented because they may be promoted to mandatory at some

	future time.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 4305	12/1/2005		
RFC 4835	4/1/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 4305	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.55) Current Dental Terminology (CDT)

General Information

Website: http://www.ada.org/ada/prod/catalog/cdt/index.asp

Description: Current Dental Terminology (CDT) is a reference manual published by the American Dental Association that contains a number of useful components, including the Code on Dental Procedures and Nomenclature (Code),

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ADA

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
CDT 2007/2008	1/1/2007		
CDT 2008/2009	1/1/2008		
CDT 2009/2010	1/1/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.56) Current Procedural Terminology (CPT)

General Information

Website: https://catalog.ama-assn.org/Catalog/product/product_detail.jsp?productId=prod1580018

Description: The Current Procedural Terminology (CPT) code set accurately describes medical, surgical, and diagnostic services and is designed to communicate uniform information about medical services and procedures among physicians, coders, patients, accreditation organizations, and payers for administrative, financial, and analytical purposes.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: AMA

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Advanced Billing Concept (ABC)
- Logical Observation Identifiers Names and Codes (LOINC)

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
January 2008	1/1/2008		
July 2008	7/1/2008		
January 2009	1/1/2009		
July 2009	7/1/2009		
January 2010	1/1/2010		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.57) Data Center

General Information

Refer to document: VA_Data_Center_Standards_1_0.pdf

Description: This standards document lists the acceptable and recommended specifications for Data Center passive Inside Plant, including racks, equipment enclosures, fiber and copper transport media, KVM, and rack-level power distribution. Sections include standard specifications for subject components, decisions supporting the standard specifications, guidelines or recommendations for implementing the standard specifications, and supplemental factors to consider when evaluating subject components. Other supplementary documents will provide guidance on procuring components that meet the standard specifications, guidance on integrating them with existing components, and explanation of how the subject components fit into the VA Architecture.

This standard includes the following: Support Infrastructure (Equipment Enclosure; Open Rack; Cable Tray; Horizontal Cable Management Panels; Vertical Cable management Panels; Fiber Distribution Cabinets); Transport Media and Interfaces (Patch Panels; Fiber Distribution Cassettes; UTP; Fiber Optic Cable; UTP Patch Cords; Fiber Patch Cords); Enclosure Power Distribution (Power Distribution Units; Zone Power Distribution Units); Remote Management Technology (KVM).

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision EIE CTO

Source:

Decision Process: TAR-TAS

Decision Date: 11/13/2009

Current Status: Analysis Completed

Introduced By: OPS/EIE

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Requirements	861: Hosting

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM

technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.58) Data Encryption Standard (DES)

General Information

Website: http://csrc.nist.gov/publications/PubsFIPSArch.html

Description: Data Encryption Standard (DES) specifies two cryptographic algorithms, the DES algorithm and the Triple Data Encryption Algorithm (TDEA) which may be used by Federal organizations to protect sensitive data. Protection of data during transmission or while in storage may be necessary to maintain the confidentiality and integrity of the information represented by the data. The algorithms uniquely define the mathematical steps required to transform data into a cryptographic cipher and also to transform the cipher back to the original form.

Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	NIST

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
FIPS 46-3	10/1/1999		5/19/2005

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
FIPS 46-3	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.59) Data Format Classification

General Information

Description: Defines the structure of a file. There are hundreds of formats, and every application has many different variations (database, word

processing, graphics, executable program, etc.). Each format defines its own layout of the data.The file format for text is the simplest.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Procedures for Establishing & Managing Privacy Act Systems of Records	VA Handbook 6300.5	This handbook sets forth procedures for establishing and managing systems of records under the Privacy Act.
Records & Information Management	VA Directive 6300	This directive provides policy for the Department of Veterans Affairs (VA) Records Management (RM) program, which includes records management, micrographics management, vital records, the Privacy Act (PA), the Freedom of Information Act (FOIA), the Computer Matching and Privacy Protection Act, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Release of Names and Addresses (RONA).
VistA Lexicon Utility		

Guidelines and Best Practices

No guidelines have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code

Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.60) Data Format for Fingerprint, Facial, & SMT Information

General Information

Website:	http://www.itl.nist.gov/ANSIASD/sp500-245-a16.pdf
Description:	ANSI/NIST-ITL: Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information defines the content, format, and units of measurement for the exchange of fingerprint, palmprint, facial/mugshot, and scar, mark, & tattoo (SMT) image information that may be used in the identification process of a subject. The information consists of a variety of mandatory and optional items, including scanning parameters, related descriptive and record data, digitized fingerprint information, and compressed or uncompressed images.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2

Decision Date: 3/14/2008
Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: NIST

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Data Format for the Interchange of Fingerprint. Part 2: XML Version	
Data Format for the Interchange of Fingerprint. Part 1	

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2000	7/27/2000		
2007	4/20/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2000	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.61) Data Integrity

General Information

Description: Data integrity is the condition where data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.
Integrity, in terms of data and network security, is the assurance that information can only be modified by those authorized to do so. Measures taken to ensure integrity include controlling the physical environment of networked terminals and servers, restricting access to data, and maintaining rigorous identification, authentication, and authorization practices. Data integrity can also be threatened by environmental hazards, such as heat, dust, water, and electrical surges.
Practices followed to protect data integrity in the physical environment include: making servers accessible only to network administrators; keeping transmission media (such as cables and connectors) covered and protected to ensure that they cannot be tapped; and protecting hardware and storage media from power surges, electrostatic discharges, and magnetism.
Network administration measures to ensure data integrity include: maintaining current authorization levels for all users, documenting system administration procedures, parameters, and maintenance activities, and creating disaster recovery plans for occurrences such as power outages, server failure, and virus attacks.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description

NIST FIPS 113	Computer Data Authentication
NIST SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
NSA - Network Security Guide	The 60 Minute Network Security Guide

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.62) Data Oriented Sites

General Information

Description: These services provide the ability to interact with a data repository based on a client's request. Typically, these services are used to dynamically generate a site's content or to enter a user's non-transactional input into a database. However, the logic associated with this service should be limited to data validation, database retrieval SQL, or "gluing" component logic together.

Decision: Approved

Decision No constraints have been specified at this time.

Constraints:

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Encapsulation	Encapsulate logic in either servlets or JavaBeans. Avoid putting processing logic directly in JSPs.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	887: Dynamic Server-Side Display

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.63) Data Protocols for Multimedia Conferencing

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=T

Description: ITU-T T.120: Data Protocols for Multimedia Conferencing define a multipoint data communication service for use in multimedia conferencing environments. The purpose of ITU-T T.120 is to provide an introduction and guide to the T.120 series. ITU-T T.120 defines the T.120 architectural model and shows the interrelationships between the constituent Recommendations.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1	7/3/1996		
1.1	2/6/1998		
2	1/13/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.64) Data Protocols for Multimedia Conferencing - Generic Conference Control

General Information

Website:	http://www.itu.int/itu-t/recommendations/index.aspx?ser=T
Description:	ITU-T T.124: Data Protocols for Multimedia Conferencing - Generic Conference Control rovides a high-level framework for conference management and control of multimedia terminals and Multipoint Control Units (MCUs). It encompasses Generic Conference Control (GCC) functions such as conference establishment and termination, managing the roster of terminals participating in a conference, managing the roster of applications and application capabilities within a conference, registry services for use by applications, coordination of conference conductorship, as well as other miscellaneous functions. It depends on companion Recommendations T.122 and T.125 (MCS) and T.123 as part of the T.120 infrastructure.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2	2/6/1998		
3	1/13/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different

releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.65) Database Services

General Information

Description: Refers to a collection of information organized in such a way that a computer program can quickly select desired pieces of data. A database management system (DBMS) is a software application providing management, administration, performance, and analysis tools for databases.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Relational		Enterprise-level data shall be stored using a relational model toenforce referential integrity.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
High Availability	Enterprise-level data needing 24/7-availability under COOP should be automatically replicated across multiple data centers.
Data Services	Component services are the preferred access method to enterprise-level data especially when dealing with updateable transactions.
Normalization	Third Normal Form (3NF) is the preferred minimal normalization standard for all data.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Database/Storage	875: Database

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.66) Datatypes for DTDs (DT4DTD)

General Information

Website: http://www.w3.org/TR/dt4dtd

Description: Datatypes for DTDs (DT4DTD) allows legacy systems that may presently be unable to convert their DTD markup declarations to XML Schema, to utilize XML Schema conformant datatypes. With it, DTD creators can specify datatypes for attribute values and data content, thereby providing the foundation for a smoother future transition path.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	898: Data Types / Validation

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Extensible Markup Language (XML) - Standard
- XML Schema - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	1/13/2000		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.67) Datejs

General Information

Website:	http://code.google.com/p/datejs/
Description:	Datejs is an open source JavaScript date library used for parsing, formatting, and processing date information, including human readable dates.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v3.2
Decision Date:	8/19/2009
Current Status:	Analysis Completed
Introduced By:	ARB
Vendor Name:	Google

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	898: Data Types / Validation
Service Interface and Integration	Interoperability	899: Data Transformation

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- JavaScript - ***(required for some configurations)***
- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	11/19/2007		

VA Forecast Information (09/09/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.0	No	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo

	ne	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted
Forecast Note:													

General Analysis

Architectural Benefits

- None significant.

Architectural Risks

- None significant.

Tier Used

- Presentation Tier (Web)

Tool Type

- Tool

Tool Usage

- Runtime

General Assessment

Expected Usage:	Not defined
Assessment Type:	New
Assessment Date:	6/25/2009
Notes:	Datejs was released only once in 11/2007. Additional updates have been applied to the open source repository. They are available anonymously over http (subversion repository)
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Datejs is based on an already approved technology, JavaScript.

2.68) Diagnosis-Related Group (DRG)

General Information

Website: http://www.cms.hhs.gov/AcuteInpatientPPS/FFD/list.asp#TopOfPage

Description: Diagnosis-Related Group (DRG) is a system to classify hospital cases into one of approximately 500 groups, also referred to as DRGs, expected to have similar hospital resource use, developed for Medicare as part of the prospective payment system. DRGs are assigned by a "grouper" program based on ICD diagnoses, procedures, age, sex, discharge status, and the presence of complications or comorbidities.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: CMS

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
25	10/1/2007		
26	10/1/2008		
27	10/1/2009		

VA Forecast Information (09/09/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.69) Diagnostic and Statistical Manual of Mental Disorders (DSM)

General Information

Website: http://www.psych.org/MainMenu/Research/DSMIV.aspx

Description: The Diagnostic and Statistical Manual of Mental Disorders (DSM) provides a common language and standard criteria for the classification of mental disorders.

The DSM organizes each psychiatric diagnosis into five levels (axes) relating to different aspects of disorder or disability:

- Axis I: Clinical disorders, including major mental disorders, and learning disorders
- Axis II: Personality disorders and mental retardation
- Axis III: Acute medical conditions and physical disorders
- Axis IV: Psychosocial and environmental factors contributing to the disorder
- Axis V: Global Assessment of Functioning or Children's Global Assessment Scale for children and teens under the age of 18

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: APA

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- International Classification of Diseases (ICD) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
DSM-IV	1/1/1994		
DSM-IV TR	7/1/2000		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
DSM-IV TR	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.70) Differentiated Services (DS) Field in IPv4 and IPv6 Headers

General Information

Website: http://tools.ietf.org/html/rfc2474

Description: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers defines the IP header field, called the DS (for differentiated services) field. In IPv4, it defines the layout of the TOS octet; in IPv6, the Traffic Class octet. In addition, a base set of packet forwarding treatments, or per-hop behaviors, is defined.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008
Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2474	12/1/1998		
RFC 3168	9/1/2001		
RFC 3260	4/1/2002		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2474	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.71) Digital Compression and Coding of Continuous-Tone Still Images

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18902

Description: ISO/IEC 10918-1 & ITU-T T.81: Digital Compression and Coding of Continuous-Tone Still Images – Requirements and Guidelines specifies processes for converting source image data to compressed

image data, processes for converting compressed image data to reconstructed image data, coded representations for compressed image data, and gives guidance on how to implement these processes in practice. Is applicable to continuous-tone - grayscale or colour - digital still image data and to a wide range of applications which require use of compressed images. Is not applicable to bi-level image data.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1	9/18/1992		
1.1	1/30/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.72) Digital Imaging and Communications in Medicine (DICOM)

General Information

Website: http://www.nema.org/stds/dicom.cfm

Description: DICOM (Digital Imaging and Communications in Medicine) enables the transfer of medical images in a multi-vendor environment and facilitates the development and expansion of picture archiving and communication systems.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: NEMA

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2006	4/24/2006		
2007	12/28/2006		
2008	1/26/2008		
2009	1/9/2010		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.73) Digital Signature

General Information

Description: A Digital Signature is a Cryptographic process used to assure message originator authenticity, integrity, and non-repudiation.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
NIST SP 800-2	Public-Key Cryptography
NIST SP 800-21	Guideline for Implementing Cryptography in the Federal Government
NIST SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication

FEA Categories

Service Area	Service Category	Service Standard Code

Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.74) Digital Signature Standard (DSS)

General Information

Website:	http://csrc.nist.gov/publications/PubsFIPS.html
Description:	FIPS 186: Digital Signature Standard (DSS) specifies a suite of algorithms that can be used to generate a digital signature. Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation, since the signatory cannot easily repudiate the signature at a later time.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2

Decision Date: 3/14/2008
Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: NIST

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	884: Certificates / Digital Signature

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2	1/1/2000		6/10/2009
3	6/10/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.75) Directory Server

General Information

Website: http://www.sun.com/software/products/directory_srvr_ee/dir_srvr/index.xml

Description: The Directory Server, formerly known as the Sun Java System Directory Server, is a scalable LDAP data store for identity information.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center

	Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	Oracle

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Simple Object Access Protocol (SOAP) related as: (Companion)
- Lightweight Directory Access Protocol (LDAP) related as: (Companion)
- Hypertext Transfer Protocol (HTTP) related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5.2	6/6/2003		
6.0	3/1/2007		
6.2	9/1/2007		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
6.2	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.76) Discovery Services

General Information

Description: Directory services help people and applications find the names and addresses of objects and services available to an application. Directory services implemented across an enterprise enable people to find destination recipients in other organizations. Directory services can be connected to the entire VA and can store information such as names of users; organizations; network resources; mailbox addresses; and message distribution lists. Interoperability among external computer systems is supported through compliance with international directory services and standards protocols.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
LDAP		Directory Services shall run a native Lightweight Directory Services Protocol (LDAP) Directory Server running directly over TCP to a database acting as a backend to another server.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Applicability	The Directory can be used as a repository for many kinds of information. The full power of DAP is unnecessary for applications that require simple read access to a few attribute values. Applications addressing is a good

	example of this type of use where an application entity needs to determine the Presentation Address (PA) of a peer entity given that peer's Application Entity Title (AET). If the AET is a Directory Name (DN), then the required result can be obtained from the PA attribute of the Directory entry as identified by the AET. This is very similar to DNS.
LDAP vs. X.500	LDAP is preferred to full X.500 services.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	Discovery Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.77) Diskeeper

General Information

Website: http://www.diskeeper.com/diskeeper/diskeeper.aspx

Description: Diskeeper is a file system defragmenter.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	Diskeeper Corp.

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Business Logic	891: Platform Dependent Technologies

Operating Systems Supported

- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2007			
2008			
2009			
2010			

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2008	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.78) Domain Name Service

General Information

Description: The VA requires a mechanism that maps domain names to IP addresses for end systems to communicate easily within the VA network. The Domain Name Service (DNS) allows network devices

to be identified and configured with a descriptive domain name.

Network resources like routers, servers, and workstations can be identified with a host name, instead of an IP address. Domain names are part of the machine name used in e-mail addresses and in host names. DNS maps host names and domain names to IP addresses. Since domain names are alphabetic, they are easier to remember. The conversion from domain name to IP addresses is essential because the computer needs to process numeric information to complete the transaction.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Configuration	Configure DNS within the operating system or application residing at the middleware layer.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	Domain Name Service*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.79) Domain Name System (DNS) Configuration Options

General Information

Website:	http://tools.ietf.org/html/rfc3646
Description:	DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6) describes options for passing a list of available DNS recursive name servers and a domain search list to a client.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3646	12/1/2003		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 3646	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.80) Domain Name System (DNS) Extensions

General Information

Website: http://tools.ietf.org/html/rfc3596

Description: Domain Name System (DNS) Extensions to Support IP Version 6 (IPv6) defines the changes that need to be made to the Domain Name System (DNS) to support hosts running IP version 6 (IPv6). The changes include a resource record type to store an IPv6 address, a domain to support lookups based on an IPv6 address, and updated definitions of existing query types that return Internet addresses as part of additional section processing. The extensions are designed to be compatible with existing applications and, in particular, DNS implementations themselves.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	Domain Name Service*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3596	10/1/2003		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 3596	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.81) Domain Name System (DNS) Structure and Delegation

General Information

Website: http://tools.ietf.org/html/rfc1591

Description: Domain Name System Structure and Delegation provides some information on the structure of the names in the Domain Name System (DNS), specifically the top-level domain names; and on the administration of domains. The Internet Assigned Numbers Authority (IANA) is the overall authority for the IP Addresses, the Domain Names, and many other parameters, used in the Internet. The day-to-day responsibility for the assignment of IP Addresses, Autonomous System Numbers, and most top and second level Domain Names are handled by the Internet Registry (IR) and regional registries.

Decision: Approved

Decision No constraints have been specified at this time.

Constraints:

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	Domain Name Service*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 1591	3/1/1994		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 1591	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.82) Dynamic Host Configuration Protocol (DHCP)

General Information

Website: http://tools.ietf.org/html/rfc2131

Description: The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCPIP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network

addresses and additional configuration options. DHCP captures the behavior of BOOTP relay agents, and DHCP participants can interoperate with BOOTP participants.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2131	3/1/1997		
RFC 3396	11/1/2002		
RFC 4361	2/1/2006		
RFC 5494	4/1/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2131	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.83) Dynamic Host Configuration Protocol Configuration of IPsec Tunnel Mode (DHCPv4)

General Information

Website:	http://tools.ietf.org/html/rfc3456
Description:	Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode explores the requirements for host configuration in IPsec tunnel mode, and describes how the Dynamic Host Configuration Protocol (DHCPv4) may be leveraged for configuration. In many remote access scenarios, a mechanism for making the remote host appear to be present on the local corporate network is quite useful. This may be accomplished by assigning the host a "virtual" address from the corporate network, and then tunneling traffic via IPsec from the host's ISP-assigned address to the corporate security gateway. In IPv4, DHCP provides for such remote host configuration.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3456	1/1/2003		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010	CY2011	CY2012

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 3456	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.84) Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

General Information

Website: http://tools.ietf.org/html/rfc3315

Description: The Dynamic Host Configuration Protocol (DHCP) for IPv6 enables DHCP servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes. It offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3315	7/1/2003		
RFC 4361	2/1/2006		
RFC 5494	4/1/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the

responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 3315	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.85) Dynamic Server Side Display

General Information

Description: This consists of the software that is used to create graphical user interfaces with the ability to change while the program is running.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Network Delivered Applications - ActiveX controls		Web browsers shall not be permitted to download untrusted ActiveX controls that can access or modify resources (external to the browser) of the local machine.
Network Delivered Applications - applets		Web browsers shall not be permitted to download unsigned applets that can access or modify resources (external to the browser) of the local machine.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Simple interactions	JavaScript should be used for relatively simple interactions (i.e. forms validation, interactive menus, etc.)
Network delivered applications	Java applets should be used for complex network delivered applications.
Platform independence	Web based client-side services should be used unless their interactive capabilities are too restrictive for a particular application.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	887: Dynamic Server-Side Display

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.86) Dynamic Updates in the Domain Name System (DNS UPDATE)

General Information

Website:	http://tools.ietf.org/html/rfc2136
Description:	The Domain Name System was originally designed to support queries of a statically configured database. While the data was expected to change, the frequency of those changes was expected to be fairly low, and all updates were made as external edits to a zone's Master File. Using this specification of the UPDATE opcode, it is possible to add or delete RRs or RRsets from a specified zone. Prerequisites are specified separately from update operations, and can specify a dependency upon either the previous existence or nonexistence of an RRset, or the existence of a single RR.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	Domain Name Service*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2136	4/1/1997		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010	CY2011	CY2012

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2136	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.87) ebXML Collaboration Protocol Profile and Agreement (ebXML CPPA)

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39972

Description: ISO/TS 15000-1 & OASIS: ebXML Collaboration Protocol Profile and Agreement (ebXML CPPA) specifies the requirements for a collaboration-protocol profile (CPP), and a collaboration-protocol agreement (CPA). The CPP describes a trading partner's technical capabilities for performing electronic business. The CPA describes the agreement between two trading partners on the technical capabilities they will use for a specific electronic-business collaboration.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- ebXML Messaging Service (ebMS) - Standard
- Uniform Resource Identifiers (URI) - Standard
- Security Assertion Markup Language (SAML) - Standard
- Extensible Markup Language (XML) - Standard
- XML Namespaces (XML-NS) - Standard
- XML Schema - Standard
- XML Pointer Framework - Standard
- XLink - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2004	1/1/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2004	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.88) ebXML Messaging Service (ebMS)

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39973

Description: ISO/TS 15000-2 & OASIS: ebXML Messaging Service (ebMS) addresses the requirements for an ebXML message service handler for the eBusiness community. ebMS defines a communications-protocol neutral method for exchanging electronic business messages and defines specific enveloping constructs supporting reliable, secure delivery of business information. ebMS includes a

flexible enveloping technique permitting messages that is independent of the payload, the communications protocol used, and also of any format type.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Core Features 3.0	This document is the specification of the core features of ebMS.
Conformance Profiles 3.0	This document is a non-normative supplement to the ebMS specification. It defines some conformance profiles that support specific messaging styles or context of use.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- WS-Reliable Messaging

Companion Technologies/Standards:

- Simple Object Access Protocol (SOAP) - Standard
- WS-Security - Standard
- Extensible Markup Language (XML) - Standard
- Uniform Resource Identifiers (URI) - Standard
- XML Namespaces (XML-NS) - Standard
- XML Schema - Standard
- XML Path Language (XPath) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2.0	4/1/2002		
3.0	7/12/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
3.0	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

Forecast Note:	

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.89) ebXML Registry Information Model (ebRIM)

General Information

Website:	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39974
Description:	ISO/TS 15000-3 & OASIS: The ebXML Registry Information Model (ebRIM) defines the requirements for the information model for the ebXML registry. The ebXML registry describes objects that reside in a repository for storage and safekeeping. The information model does not deal with the actual content of the repository. All elements of the information model represent metadata about the content stored in the repository. Such information is used to facilitate ebXML-based Business-to-Business partnerships and transactions. The registry information model provides a high-level schema for the ebXML registry. It provides information on the type of metadata that are stored in the registry as well as the relationships among metadata classes. The registry information model defines what types of objects are stored and defines how stored objects are organized. The abstract registry is implemented using one or both of the following concrete bindings: a SOAP binding using the HTTP protocol, or an ebXML messaging service binding. These specifications are compatible with other ebXML specifications.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed

Introduced By: TRMSP

Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interface	900: Service Discovery

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- ebXML Registry Services (ebRS) - Standard
- ebXML Collaboration Protocol Profile and Agreement (ebXML CPPA) - Standard
- XML Path Language (XPath) - Standard
- XML Namespaces (XML-NS) - Standard
- Extensible Markup Language (XML) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2004	1/1/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2004	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.90) ebXML Registry Services (ebRS)

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39975

Description: ISO/TS 15000-4 & OASIS: Electronic business eXtensible Markup Language Registry services (ebRS) defines the interface between the registry and the registry clients, as well as the interaction protocols, message definitions and XML schema.

Decision: Approved

Decision No constraints have been specified at this time.

Constraints:

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
ebXML Registry Services and Protocols	This document defines the services and protocols for an ebXML Registry.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interface	900: Service Discovery

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Universal Description, Discovery, and Integration (UDDI)

Companion Technologies/Standards:

- Extensible Markup Language (XML) - Standard
- Security Assertion Markup Language (SAML) - Standard
- Simple Object Access Protocol (SOAP) - Standard
- Structured Query Language (SQL) - Standard
- WS-I Basic Profile - Standard
- XML Path Language (XPath) - Standard
- XML Namespaces (XML-NS) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2004	1/1/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2004	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.91) Eclipse

General Information

Website:	http://www.eclipse.org
Description:	Eclipse is an open source (supported by IBM) integrated development environment composed of frameworks and common services. Plug-ins must be loaded, integrated and executed in order to equip Eclipse to handle Java software development. Eclipse is an open framework that has uses beyond that of a Java development environment. Eclipse forms the foundation for the Rational development tools offered by Enterprise Tools Management. The Rational tools should be utilized unless there is a compelling reason to deviate from the standard.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	Eclipse

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	867: Integrated Development Environments (IDE)

Operating Systems Supported

- Red Hat Linux
- Windows (Client)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***
- XSL Transformations (XSLT) - ***(required for some configurations)***

Comparable Technologies/Standards:

- Rational Software Architect
- MyEclipse
- Rational Systems Developer
- Rational Application Developer

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.2	6/30/2006		
3.3	6/29/2007		
3.4	6/25/2008		
3.5	6/24/2009		
3.6 (est)	6/30/2010		

VA Forecast Information (09/29/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
3.3	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
3.4	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
3.5	None	None	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment development utilizing Eclipse is currently based on version 3.3.

General Analysis

Architectural Benefits

- Eclipse provides a flexible and extensible integrated development environment for coding Java Standard Edition and Java Enterprise Edition applications.

Architectural Risks

- Eclipse does not provide all of the tools needed for Java development, requiring end-users to locate, download, and install additional components. This can lead to compatibility issues and a non-functioning environment if not performed carefully.

Tool Type

- Platform
- Framework
- Tool

Tool Usage

- Development

General Assessment

Expected Usage:	Provide developers with an extensible Java-integrated development environment.
Assessment Type:	Refresh
Assessment Date:	11/10/2008
Notes:	Eclipse provides a solid foundation for a Java-integrated development environment, and forms the foundation for the Rational development tools (RSA, RAD) offered by Enterprise Tools Management. The Rational tools should be utilized unless there is a compelling reason to deviate from the standard.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Recommend approval for development teams currently productive with Eclipse. New projects should be using the tool baseline as specified by Enterprise Tools Management.

2.92) Eclipse Modeling Framework (EMF)

General Information

Website:	http://www.eclipse.org/modeling/emf/
Description:	Eclipse Modeling Framework (EMF) is a Java code generation package for building tools and applications based on a structured model. The model can be built using XMI (XML Metadata Interchange), annotated Java structures, or an XML Schema.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v3.2
Decision Date:	8/19/2009
Current Status:	Assessment Complete
Introduced By:	ARB
Vendor Name:	Eclipse

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	867: Integrated Development Environments (IDE)

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- JAXB Reference Implementation

Companion Technologies/Standards:

- Eclipse related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2.3.2	2/5/2008		
2.4.0	6/9/2008		
2.4.1	8/25/2008		
2.4.2	2/17/2009		
2.5.0	6/15/2009		

VA Forecast Information (09/09/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2.4.2	None	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
2.5.0	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

Forecast Note:	Eclipse is only required to use EMF's tools. For runtime-only use, only a JRE is required.

General Analysis

Adoption Benefits

- The validation components of EMF provide capabilities to ensure structured model integrity.

Adoption Risks

- None significant.

Architectural Benefits

- The use of EMF will facilitate well-documented object models and validated model integrity; this should reduce run-time errors and provide for improved error correction.

Architectural Risks

- None significant.

Standards Traceability

- XMI 2.0 Specification

General Assessment

Expected Usage:	EMF provides tools-runtime support to produce a set of Java classes from models, along with a set of Java classes that enable viewing and command-based editing of the model.
Assessment Type:	New
Assessment Date:	6/10/2009
Notes:	
Recommendation:	Approve
Recommendation Constraints:	None
Recommendation Justification:	The Eclipse Modeling Framework has already deployed as a component of the Rational development tool suite. The Health Data Repository has been using EMF under a waiver without issue. The run-time components of EMF function in the Java sandbox and are as safe as any Java components from the Eclipse project.

2.93) eGate Integrator

General Information

Website:	http://developers.sun.com/javacaps/product_list.html#1
Description:	eGate Integrator is a J2EE technology-compliant and web-services-based distributed integration platform. eGate Integrator provides core integration including comprehensive systems connectivity, guaranteed messaging, and robust transformation capabilities. It also provides a unified, single sign-on environment for integration development, deployment, monitoring and management.

Decision:	Approved
Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	Oracle

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	896: Enterprise Application Integration

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- BusinessWare
- Mirth Connect

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5.1	7/19/2006		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
5.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.94) Electronic Authentication of Health Care Information

General Information

Website: http://www.astm.org/Standards/E1762.htm

Description: ASTM E1762: Standard Guide for Electronic Authentication of Health Care Information defines:

- a document structure for use by electronic signature mechanisms
- the characteristics of an electronic signature process
- the minimum requirements for different electronic signature mechanisms
- the signature attributes for use with electronic signature mechanisms
- acceptable electronic signature mechanisms and technologies
- minimum requirements for user identification, access control, and other security requirements for electronic signatures
- technical details for all electronic signature mechanisms in sufficient detail to allow interoperability between systems supporting the same signature mechanism

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ASTM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
95(2003)	1/1/2003		
95(2009)	1/1/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be

supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
95(2003)	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.95) Encryption Algorithm and IPsec

General Information

Website: http://tools.ietf.org/html/rfc2410

Description: The NULL Encryption Algorithm and Its Use With IPsec defines the NULL encryption algorithm and its use with the IPsec Encapsulating Security Payload (ESP) to provide authentication and integrity without confidentiality.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2410	11/1/1998		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different

releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2410	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.96) Encryption Services

General Information

Description: Encryption services use cryptographic algorithms to encode clear text to prevent anyone other than the intended recipient(s) from reading that data. Encryption services are utilized innumerous information protection mechanisms and in infrastructure components required tosupport these mechanisms, such as data at rest encryption, e-mail encryption, and WorldWide Web (WWW) encryption.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
SSL		Servers that use SSL shall be configured to only enable SSL v3.
Data Storage		Data at rest encryption products shall only employ products that use the symmetric data encryption algorithm AES. Other symmetric encryption algorithms require prior approval before use.
Encryption		Adherence to NIST FIPS 140-2 – Security Requirements for Cryptographic Modules is required when using cryptography for Privacy.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
E-mail Encryption	E-mail encryption should be deployed as S/MIME-based solutions. PKI supports trusted digital signatures in S/MIME messages and should be used to implement e-mail encryption.
ISO/IEC 10181-4	Non-repudiation Framework
ISO/IEC 10181-5	Confidentiality Framework

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.97) Enhanced Security Services for S/MIME

General Information

Website: http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

Description: Enhanced Security Services for S/MIME describes four optional security service extensions for S/MIME. The services are:

- signed receipts
- security labels
- secure mailing lists
- signing certificates

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2634	6/1/1999		
RFC 5035	8/1/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2634	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.98) Environmental Protection Agency - Substance Registry System (EPA-SRS)

General Information

Website: http://iaspub.epa.gov/sor_internet/registry/substreg/home/overview/home.do

Description: Substance Registry Services (SRS) is the Environmental Protection Agency's (EPA) central system for information about substances that are tracked or regulated by EPA or other sources. It is the authoritative resource for basic information about chemicals, biological organisms, and other substances of interest to EPA and its state and tribal partners.

The SRS makes it possible to identify which EPA data systems, environmental statutes, or other sources have information about a substance and which synonym is used by that system or statute. It becomes possible therefore to map substance data across EPA programs regardless of synonym.

The system provides a common basis for identification of, and information about:

- Chemicals
- Biological organisms
- Physical properties
- Miscellaneous objects

Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	EPA

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.99) ERwin Data Modeler

General Information

Website: http://www.ca.com/us/data-modeling.aspx

Description: ERwin Data Modeler is a is a software tool for data modeling (data requirements analysis, database design etc) of custom developed information systems, including databases of transactional systems and data marts

Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	HSD&D
Decision Process:	ETL
Decision Date:	12/1/2006
Current Status:	Introduced
Introduced By:	Extended Tool List (ETL)
Vendor Name:	CA

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	870: Modeling

Operating Systems Supported

- Windows (Client)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
r7.2	5/3/2007		
r7.3	1/26/2009		

VA Forecast Information (09/09/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
r7.2	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
r7.3	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

ETL Approved Technology/Standard, TRM Analysis still pending.

General Assessment

ETL Approved Technology/Standard, TRM Assessment still pending.

2.100) Escrowed Encryption Standard

General Information

Website: http://csrc.nist.gov/publications/PubsFIPS.html

Description: FIPS 185: This standard specifies an encryption/decryption algorithm and a Law Enforcement Access Field (LEAF) creation method which may be implemented in electronic devices and used for protecting government telecommunications when such protection is desired. The algorithm and the LEAF creation method are classified and are referenced, but not specified, in the standard. Electronic devices implementing this standard may be designed into cryptographic modules which are integrated into data security products and systems for use in data security applications. The LEAF is used in a key escrow system that provides for decryption of telecommunications when access to the telecommunications is lawfully authorized.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: NIST

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1	2/9/1994		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.101) Establishing Communication Between Multiple Audiovisual Terminals

General Information

Website:	http://www.itu.int/itu-t/recommendations/index.aspx?ser=H
Description:	ITU-T H.243: Procedures for establishing communication between three or more audiovisual terminals using digital channels up to 1920 kbit/s identifies the system operation for a conference call between three or more audiovisual terminals conforming to ITU-T H.320.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5	10/7/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
5	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.102) European Article Number (EAN-13)

General Information

Website: http://www.gs1.org/barcodes

Description: European Article Number (EAN-13) barcode is a barcoding standard which is a superset of the original 12-digit Universal Product Code (UPC) system developed in the United States.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: GS1

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is

considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.103) Exchange Server

General Information

Website: http://www.microsoft.com/exchange/

Description: Exchange Server is the server side of a client-server, collaborative application product. Its major features consist of electronic mail, calendaring, contacts and tasks; support for mobile and web-based access to information; and support for data storage.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: CDCO Supported Architecture Components

Vendor Name: Microsoft

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Access Channels	852: Collaboration / Communications

Operating Systems Supported

- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Active Directory - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Secure/Multipurpose Internet Mail Extensions (S/MIME) Message Spec related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2003	9/28/2000		
2007	11/30/2006		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the

responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2003	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.104) Extended Simple Mail Transfer Protocol (ESMTP)

General Information

Website: http://tools.ietf.org/html/rfc1870

Description: Extended Simple Mail Transfer Protocol (ESMTP) defines an extension to the SMTP service whereby an SMTP client and server may interact to give the server an opportunity to decline to accept a message (perhaps temporarily) based on the client's estimate of the message size.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 1870	11/1/1995		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 1870	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.105) eXtensible Access Control Markup Language (XACML)

General Information

Website: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

Description: The eXtensible Access Control Markup Language (XACML) specification defines an XML schema for an extensible access-control policy language.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008
Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: OASIS

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Access Control Framework - Standard
- Lightweight Directory Access Protocol (LDAP) - Standard
- Uniform Resource Identifiers (URI) - Standard
- Security Assertion Markup Language (SAML) - Standard
- XML Path Language (XPath) - Standard
- XSL Transformations (XSLT) - Standard
- XML Schema - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	2/18/2003		
1.1	7/24/2003		
2.0	2/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.106) Extensible Authentication Protocol (EAP)

General Information

Website: http://tools.ietf.org/html/rfc5247

Description: Extensible Authentication Protocol (EAP) is an authentication

framework which supports multiple authentication methods. EAP typically runs directly over data link layers such as Point-to-Point Protocol (PPP) or IEEE 802, without requiring IP. EAP provides its own support for duplicate elimination and retransmission, but is reliant on lower layer ordering guarantees.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3748	6/1/2004		
RFC 5247	8/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 3748	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.107) Extensible Authentication Protocol Tunneled Transport Layer Security (EAP-TTLS)

General Information

Website:	http://tools.ietf.org/html/rfc5281
Description:	Extensible Authentication Protocol Tunneled Transport Layer Security (EAP-TTLS) is an EAP (Extensible Authentication Protocol) method that encapsulates a TLS (Transport Layer Security) session, consisting of a handshake phase and a data phase. During the handshake phase, the server is authenticated to the client (or client and server are mutually authenticated) using standard TLS procedures, and keying material is generated in order to create a cryptographically secure tunnel for information exchange in the subsequent data phase. During the data phase, the client is authenticated to the server (or client and server are mutually authenticated) using an arbitrary authentication mechanism encapsulated within the secure tunnel. The encapsulated authentication mechanism may itself be EAP, or it may be another authentication protocol such as PAP, CHAP, MS-CHAP, or MS-CHAP-V2. Thus, EAP-TTLS allows legacy password-based authentication protocols to be used against existing authentication databases, while protecting the security of these legacy protocols against eaves dropping, man-in-the-middle, and other attacks. The data phase may also be used for additional, arbitrary data exchange.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Transport Layer Security (TLS) Protocol - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 5281	8/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is

considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 5281	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.108) Extensible HyperText Markup Language (XHTML)

General Information

Website: http://www.w3.org/TR/

Description: This specification defines XHTML, a reformulation of HTML as an XML application, and three DTDs; Strict, Transitional, and Frameset. These DTDs correspond to the ones defined by HTML. The semantics of the elements and their attributes provide the foundation for future extensibility of XHTML. Compatibility with existing HTML user agents is possible by following a small set of guidelines.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Namespace	XHTML Strict should be used as the preferred namespace.

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	888: Content Rendering

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- HyperText Markup Language (HTML) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	1/26/2000		
1.1	5/31/2001		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.109) Extensible Markup Language (XML)

General Information

Website: http://www.w3.org/TR/

Description: The Extensible Markup Language (XML) is a subset of SGML that is completely described in the specification. Its goal is to enable generic SGML to be served, received, and processed on the Web in the way that is now possible with HTML. XML has been designed for ease of implementation and for interoperability with both SGML and HTML.

Decision: Approved

Decision Constraints:	No constraints have been specified at this time.
Decision Source:	Benefits Arch
Decision Process:	TRM v4.1
Decision Date:	10/28/2009
Current Status:	Analysis Completed
Introduced By:	Benefits ASA
Vendor Name:	W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Federal XML Developer's Guide	This document is an early deliverable of the overall federal strategy for employing XML.
XML Document Structure	XSDs are preferred for describing the structure of XML documents over DTDs.

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	2/10/1998		
1.1	9/29/2006		

VA Forecast Information (10/05/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.0	None	None	None	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
1.1	None	None	None	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. The Benefits Segment use of the XML specification is currently based on version 1.0.

General Analysis

Adoption Benefits

- Openness: A mature, widely adopted industry standard
- Enables the adoption of many other standards that are XML based
- Simplicity - information coded in XML is easy to read and understand

Architectural Benefits

- Internationalization - supports multilingual documents and Unicode
- Interoperability - platform, protocol, and network independent
- Self-description - XML documents contain meta data in the form of tags and attributes
- A common data representation for all levels of the architecture
- Extensibility - new tags can be created as needed
- Facilitates the comparison and aggregation of data

Architectural Risks

- Its expanded size compared with a binary format has an impact on performance

Tier Used

- Client Tier
- Data Tier
- Middle Tier (Integration)
- Middle Tier (Infrastructure)
- Middle Tier (Business)

Tool Usage

- Runtime
- Development

General Assessment

Expected Usage:	XML is a data format standard.
Assessment Type:	Standard
Assessment Date:	11/2/2009
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	XML is a mature, widely adopted industry standard that greatly improves interoperability. It is a core standard upon which many industry standards are based.

2.110) Fault Management

General Information

Description: Fault management describes the process of preventing, isolating, diagnosing and resolution of problems when they occur. To ensure that critical information is always available at the right place and time, fault management services provide the capability to monitor and detect fault conditions. Fault management can provide the capability for restarting failed processes, and switching over to a secondary device or site, in the event the primary device or site becomes inoperable. A goal of fault management is to ensure COOP and provide rapid network recovery within any defined and agreed upon maximum downtime.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Network Management		The network management system shall display management data, monitor and control managed devices, and communicate with management agents. Data link and physical layer parameters shall be monitored by management systems that are based on Management Information Base (MIB) - Remote Monitoring (RMON) standards.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Management Device	A router, server, switch, or end system should be selected on each network to be a local management device.
Problem Notification	Users should be informed about ongoing problems, and given a timeframe for resolution.
Problem Resolution Documentation	After a problem is resolved, the problem/resolution should be tested and then documented in a problem-tracking database.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.111) FDR

General Information

Website: http://www.fdr.com/products/fdrabr/

Description: FDR provides standard, high-performance, “non-managed” volume and data set backup and restore services.

Decision: Approved

Decision Constraints: This technology’s assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center

	Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	Innovation

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- z/OS

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- NetBackup

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5.4			

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
5.4	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.112) Fiber Distributed Data Interface (FDDI)

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=16973

Description: ISO/IEC 9314: Fiber Distributed Data Interface (FDDI) provides a 100Mbps optical standard for data transmission in a local area network that can extend in range up to 200 kilometers (124 miles).

Although FDDI logical topology is a ring-based token network, it does not use the IEEE 802.5 token ring protocol as its basis; instead, its protocol is derived from the IEEE 802.4 token bus timed token protocol. In addition to covering large geographical areas, FDDI local area networks can support thousands of users. As a standard underlying medium it uses optical fiber, although it can use copper cable, in which case it may be refer to as CDDI. FDDI offers both a Dual-Attached Station (DAS), counter-rotating token ring topology and a Single-Attached Station (SAS), token bus passing ring topology.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Token Ring Physical Layer Protocol (PHY)	This document defines the Physical Layer Protocol (PHY), the upper sublayer of the Physical Layer, for Fibre Distributed Data Interface (FDDI).
Token Ring Media Access Control (MAC)	This document describes the Media Access Control (MAC), the lower sublayer of the Data Link Layer (DLL), for Fibre Distributed Data Interface (FDDI).
Physical Layer Medium Dependent (PMD)	This document defines the structure of the FDDI and specifies the functions and operations necessary to insure interoperability between conforming FDDI

	implementations.
Single Mode Fibre Physical Layer Medium Dependent (SMF-PMD)	
Hybrid Ring Control (HRC)	
Station Management (SMT)	
Physical layer Protocol (PHY-2)	
Media Access Control-2 (MAC-2)	
Low-cost fibre physical layer medium dependent (LCF-PMD)	
Conformance Test Protocol Implementation Conformance Statement (CT-PICS) Proforma	
Abstract test suite for FDDI physical medium dependent conformance testing (FDDI PMD ATS)	

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	Campus Area Network (CAN)*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1989			
1990			
1995			
1998			
1999			
2000			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2000	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.113) File Transfer Protocol (FTP)

General Information

Website: http://tools.ietf.org/html/rfc959

Description: File Transfer Protocol (FTP) is a standard network protocol used to exchange and manipulate files over a TCP/IP-based network, such as the Internet. FTP is built on a client-server architecture and utilizes separate control and data connections between the client and server applications. FTP is used with user-based password authentication or with anonymous user access.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Hypertext Transfer Protocol (HTTP)

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 959	10/1/1985		
RFC 2228	10/1/1997		
RFC 2640	7/1/1999		
RFC 2773	2/1/2000		
RFC 3659	3/1/2007		
RFC 5759	3/1/2010		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 959	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.114) File Transfer Protocol (FTP) Extensions

General Information

Website:	http://tools.ietf.org/html/rfc2428
Description:	File Transfer Protocol (FTP) Extensions for IPv6 and Network Address Translators (NATs) specifies extensions to FTP that will allow the protocol to work over IPv4 and IPv6. In addition, the framework defined can support additional network protocols in the future.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2428	9/1/1998		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**

RFC 2428	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.115) File Transfer Protocol Services

General Information

Description:	File Transfer Protocol (FTP) Services are the portion of a server that listens on a port for FTP requests. The default port is 21.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.116) Fire Walling

General Information

Description:	A firewall is a system designed to prevent unauthorized access to or from a different parts of a network architecture. In addition to providing network access control, a properly configured and managed firewall can provide network intrusion prevention and limit damage caused by any single intrusion or security event.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
VA Firewall Policy	VA Memorandum Aug 29, 2001	Attachment to the VA Assistant Secretary for Information Technology Memorandum of August 29, 2001 “Securing the Department’s Information Technology Infrastructure”

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Layer Gateway Network Firewalls	All information systems should use application layer gateway network firewalls to secure connections to public networks. Network firewalls can be centrally located, centrally managed,and shared between multiple sites only if a secure intranet is used to connect the sites.
Default Restrictive Policy	Network firewalls should be configured with the most restrictive security policy possible, “thatwhich is not expressly allowed is denied.”
Network Firewalls Compatibility	Information systems should ensure that any protocols used across public inter-networks arecompatible with application layer gateway network firewalls.
Host-based Firewalls	Host-based firewalls should be used on: Large web portals or web farms, servers that provide critical services, i.e., database servers, e-mail servers, etc., and services that process and store critical or proprietary information, i.e., payroll,accounting, human resources, etc.
Personal Firewalls	Personal firewalls should be used on all client workstations. Personal firewalls on client workstations should be centrally managed.
NIST SP 800-41	Guidelines on Firewalls and Firewall Policy

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.117) Firefox

General Information

Website:	http://www.mozilla.com/en-US/
Description:	Firefox is a widely utilized Web browser. It provides access to HeV thin client applications and serves as the operating environment for Web based client side components.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	TRM Team
Vendor Name:	Mozilla

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code

Service Access and Delivery	Access Channels	850: Web Browser

Operating Systems Supported

- Red Hat Linux
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required for some configurations)***
- XSL Transformations (XSLT) - ***(required for some configurations)***

Comparable Technologies/Standards:

- Internet Explorer

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.5	11/29/2005	5/30/2007	
2.0	10/24/2006	12/18/2008	4/30/2009
3.0	6/17/2008		
3.5	6/30/2009		

VA Forecast Information (10/06/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is

considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2.0	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
3.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
3.5	None	None	Evaluation	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. The Benefits Segment use of Firefox is currently based on version 1.5.

General Analysis

Architectural Benefits

- As a modular, standards-based Web browser, Firefox will enable the scalable and flexible deployment of thin-client applications.

Architectural Risks

- The introduction of more than one Web browser (to coexist with Internet Explorer) creates multiple versions of the JavaScript interpreter, application add-ins (plug-ins), and could result in compatibility issues for HeV developers.

EA Requirement

- ENTR 955 (Inactive) - Web browser based applications shall not require or encourage users to choose any specific browser or viewer software.

Tool Usage

- Firefox is collaborating with the Web Standards Project to identify and improve compliance with industry standards. Additional information can be found at: http://developer.mozilla.org/en/docs/Web_Standards.

General Assessment

Expected Usage: Firefox provides a standardized deployment and operational platform at the client level in the HeV architecture.

Assessment Type: Refresh

Assessment Date:	9/16/2008
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Recommend approval as an alternative Web browser.

2.118) Flex SDK

General Information

Website:	http://www.adobe.com/products/flex/
Description:	Flex is an open source framework for developing internet applications. Flex includes MXML, a markup language used for user interface layout and behavior design, ActionScript for programming logic and an extensible component library.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v4.1
Decision Date:	10/28/2009
Current Status:	Analysis Completed
Introduced By:	ARB
Vendor Name:	Adobe

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	888: Content Rendering

Operating Systems Supported

- Red Hat Linux
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- BlazeDS - ***(required for some configurations)***
- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	3/1/2004		
1.5	10/1/2004		
2.0	6/28/2006		
2.0.1	1/5/2007		
3.0	2/25/2008		
3.1	8/15/2008		
3.2	11/17/2008		
3.3	3/4/2009		

3.4	8/19/2009		
4.0 (est)	3/1/2010		

VA Forecast Information (10/06/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
3.3	None	None	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
3.4	None	None	None	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
4.0 (est)	None	None	None	None	None	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Adoption Benefits

- Flex is licensed as an open source product, however, Adobe supports and is developing the codebase with a roadmap.
- Learning curve for developers is short; online community is robust with examples and assistance.
- Built in 508 and JAWS support is provided in the component library.

Adoption Risks

- As of release 3.4, Flex can be developed using open source IDEs but the possibility of vendor lock in on Flex Builder exists.

Architectural Benefits

- None significant.

Architectural Risks

- None significant.

Tool Type

- Framework

Tool Usage

- Build Flash internet applications.

General Assessment

Expected Usage:	Internet application development.
Assessment Type:	New
Assessment Date:	10/5/2009
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	The Flex framework is an open source framework being developed and supported by Adobe systems. Flex has a large customer base and has been successfully implemented in production on a couple of VA projects.

2.119) Frame Structure in Audiovisual Teleservices

General Information

Website:	http://www.itu.int/itu-t/recommendations/index.aspx?ser=H
Description:	ITU-T H.221: Frame Structure for a 64 to 1920 kbit/s Channel in Audiovisual Teleservices defines a frame structure for audiovisual teleservices in single or multiple B or H0 channels or a single H11 or H12 channel which makes the best use of the characteristics and properties of the audio and video encoding algorithms, of the transmission frame structure and of the existing Recommendations.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA

Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM

technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
7	3/15/2004		
7.1	9/13/2005		
8	3/16/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
7.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.120) Frame-synchronous Control and Indication Signals for Audiovisual Systems

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=H

Description: ITU-T H.230: Frame-synchronous Control and Indication Signals for Audiovisual Systems details the Control and Indication (C&I) related to video and audio; means of transmitting numbers and characters;

C&I for maintenance purposes; for simple multipoint conferences not using protocol in the Meridian Lossless Packing (MLP) channel; for channel aggregation; and for the transfer of network addresses.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
6	3/15/2004		
6.1	10/7/2005		
7	3/16/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
6.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.121) General Parallel File System (GPFS)

General Information

Website: http://www-03.ibm.com/systems/software/gpfs/index.html

Description: The General Parallel File System (GPFS) is a high-performance shared-disk clustered file system. GPFS provides online storage management, scalable access, and integrated information lifecycle management tools capable of managing petabytes of data and billions of files.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: CDCO Supported Architecture Components

Vendor Name: IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Business Logic	890: Platform Independent Technologies

Operating Systems Supported

- AIX
- Red Hat Linux

- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2.3	5/1/2008		
3.1	7/1/2009		
3.2	9/1/2007		
3.3	9/1/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2.3	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated

Forecast Note:	

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.122) Google Maps

General Information

Website:	http://code.google.com/apis/maps/
Description:	The Google Maps API facilitates embedding Google Maps in Web pages using JavaScript.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v3.2
Decision Date:	8/19/2009
Current Status:	Introduced
Introduced By:	ARB
Vendor Name:	Google

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code

Component Framework	User Presentation/Interface	888: Content Rendering

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- JavaScript - ***(required libraries)***

Comparable Technologies/Standards:

- Bing Maps

Companion Technologies/Standards:

- AJAX related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2	4/3/2006		
3	2/4/2009		

VA Forecast Information (06/16/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**

2	None	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
3	None	None	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Adoption Benefits

- The graphical map view enhances applications that present location data.

Architectural Benefits

- The thin-client architecture of Google Maps fits into the HEV paradigm.

Architectural Risks

- The potential inclusion of VA information in Google search results must be closely monitored and controlled by opt-out.

General Assessment

Expected Usage: Browser-based applications that need geographical data.

Assessment Type: New

Assessment Date: 6/16/2009

Notes: Developers should be cautious about the potential for inclusion of VA content in Google search results. It is possible to opt out of Google search results, or to purchase an enterprise license that will permit the isolated use of the Maps API inside of the VA Network.

Google Maps is not 508 compliant. However, an alternative for screen readers can be presented. For example, offering a map view but also a "list view" that is screen reader friendly.

Recommendation: Approve

Recommendation Constraints: Developers must be cautious about the potential for inclusion of VA content in Google search results.

Recommendation Justification: The Google Maps API is stable with a good track record and a large installation base. This is a browser-based application without a client-side installation.

2.123) Graphics Interchange Format (GIF)

General Information

Website:	http://www.w3.org/Graphics/GIF/spec-gif89a.txt
Description:	The Graphics Interchange Format defines a protocol intended for the on-line transmission and interchange of raster graphic data in a way that is independent of the hardware used in their creation or display.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	888: Content Rendering

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1990	7/31/1990		

VA Forecast Information (06/16/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.124) Health Information Data Exchange

General Information

Description: Health Information Data Exchange standards support batch-oriented, messaging capability (i.e., orders, results,admission, discharge, transfer, etc.) between health information systems.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Application Exchange	HL7 messages should be used when the application is hosted on a PC or Server-based platform, not a micro-controller platform.
Device Exchange	The FDA has not accepted HL7 for use in regulated medical devices.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.125) Healthcare Common Procedure Coding System (HCPCS)

General Information

Website: http://www.cms.hhs.gov/HCPCSReleaseCodeSets/ANHCPCS/list.asp#TopOfPage

Description: The Healthcare Common Procedure Coding System (HCPCS) is a set of health care procedure codes based on the American Medical Association's Current Procedural Terminology (CPT). Commonly pronounced Hick-Picks.

HCPCS includes three levels of codes:
<ul
• Level I consists of the American Medical Association's Current Procedural Terminology (CPT) and is numeric.
• Level II codes are alphanumeric and primarily include non-physician services such as ambulance services and prosthetic devices[2], and represent items and supplies and non-physician services not covered by CPT-4 codes (Level I). Level II alphanumeric procedure and modifier codes are a single alphabetical letter followed by 4 numeric digits; the first alphabetic letter is in the A to V range. Level II codes are maintained by the US Centers for Medicare and Medicaid Services (CMS). There is some overlap between HCPCS codes and National Drug Code (NDC) codes, with a subset of NDC codes also in HCPCS, and vice-versa. The CMS maintains a crosswalk from NDC to HCPCS in the form of an Excel file. The crosswalk is updated quarterly.
• Level III codes, also called local codes, were developed by state

Medicaid agencies, Medicare contractors, and private insurers for use in specific programs and jurisdictions. The use of Level III codes was discontinued on December 31, 2003, in order to adhere to consistent coding standards.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: CMS

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Current Procedural Terminology (CPT) - Standard
- National Drug Code (NDC) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2008	11/1/2007		
2009	11/10/2008		
2010	11/5/2009		

VA Forecast Information (06/16/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.126) Hibernate Core

General Information

Website:	http://www.hibernate.org
Description:	Hibernate is a set of object-relational tools which provide a persistence framework for storing, retrieving and querying Java object state stored in a relational database.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	RedHat

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	895: Middleware

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Apache Commons - ***(required libraries)***
- JRE - Sun - ***(required libraries)***
- JAXP Reference Implementation - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.2.3	1/2/2007		
3.2.4	1/9/2007		
3.2.5	1/31/2007		
3.2.6	1/7/2008		
3.3.0	1/15/2008		
3.3.2	6/24/2009		
3.5 (est)			

VA Forecast Information (10/07/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008	CY2009	CY2010

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
3.2.5	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
3.3.0	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Deprecated	Deprecated
3.5 (est)	None	None	None	None	None	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Architectural Area

- Application
- Data

Architectural Benefits

- Supports the ability to rapidly respond to structural changes in the middle tier or database, and to add new persistent types with minimal programming
- Provides a consistent method of storing and retrieving java object state from a relational database.

Architectural Risks

- If Hibernate is not abstracted properly behind data services, vendor lock-in could occur.

Standards Traceability

- Java EE - JNDI 1.2.1
- Java EE - JTA 1.0.1B
- Java EE - JMX 1.5
- Java EE - EJB 3.0
- Java EE - JDBC 3.0

Tier Used

- Data Tier
- Middle Tier (Infrastructure)
- Presentation Tier (Web)

Tool Type

- Framework

Tool Usage

- Development
- Runtime - Embedded

General Assessment

Expected Usage:	Provide a robust object/relational mapping and persistence framework.
Assessment Type:	Refresh
Assessment Date:	9/5/2008
Notes:	Suggest the use of JPA versus Hibernate mappings whenever possible.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Recommend continued use of Hibernate.

2.127) HL7

General Information

Website:	http://www.hl7.org/
Description:	HL7 (Health Level Seven) specifies a number of standards, guidelines, and methodologies by which healthcare systems communicate with each other. The HL7 standards allow healthcare organizations to share clinical information in a consistent format. HL7 develops Conceptual Standards (HL7 RIM), Document Standards (HL7 CDA), Application Standards (HL7 CCOW), and Messaging Standards (HL7 V2.x and V3.0).
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision	TRM v2

Process:
Decision Date: 9/17/2008
Current Status: Analysis Completed
Introduced By: TRM Team
Vendor Name: HL7

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- VHIM

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2.3	5/13/1997		
2.3.1	4/14/1999		
2.4	10/6/2000		
2.5	6/26/2003		
2.5.1	2/21/2007		
2.6	10/12/2007		
3	8/14/2008		

VA Forecast Information (10/07/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008				CY2009				CY2010			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2.3	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
2.4	None	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
2.5	None	None	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
2.6	None	None	None	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
3	None	None	None	None	None	None	None	None	None	None	Planning	Evaluation
Forecast Note:												

General Analysis

Architectural Area

- Data

Architectural Benefits

- As the standard for health data exchange, HL7 is a must for the VA.

Architectural Risks

- VHIM may require adaptation for use with version 3 of HL7

EA Requirement

- ENTR 1074 - Implement a One VA information technology framework that supports the integration of information across business lines and that provides a source of consistent, reliable, accurate, and secure information to veterans and their families, employees, and stakeholders (Enabling Objective E-3).
- ENTR 247 - VHA Driver - HIPAA - HIPAA will standardize the interchange of electronic data for specific administrative and financial transactions and protect the security and confidentiality of electronic health information. HIPAA legislation requires that standards be adopted in the following areas: · Standards for Electronic Transactions · National Provider Identifier · Employer Identifier · National Patient Identifier · National Health Plan (Payer) Identifier · Security Standards · Code Sets (examples, disease/diagnostic, dentistry, pharmacy, procedural coding) · Privacy

Tier Used

- Business Logic Tier
- Data Tier

Tool Type

- Open Source

Tool Usage

- Development
- Runtime - Embedded

General Assessment

Expected Usage: Use HL7 version 2.x messaging, Clinical Document Architecture (CDA), and the Clinical Context Object Workgroup (CCOW) in VA IT services. Use HL7 v3 whenever the VHIM cannot fulfill project requirements, or when off-the-shelf software requires HL7 v3.

Assessment Type:	Standard
Assessment Date:	9/9/2008
Notes:	Version 3 is a radical departure from previous releases and represents a new paradigm for HL7. Version 3 uses an object-oriented development methodology and a Reference Information Model (RIM) to create messages. The RIM is an essential part of the HL7 Version 3 development methodology, as it provides an explicit representation of the semantic and lexical connections that exist between the information carried in the fields of HL7 messages.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Continue using HL7 v2.x as a standard. Use HL7 v3 whenever the VHIM cannot fulfill project requirements, or when off-the-shelf software requires HL7 v3.

2.128) HP-UX

General Information

Website:	http://h71028.www7.hp.com/enterprise/w1/en/os/hpux11i-overview.html
Description:	HP-UX (Hewlett Packard UniX) is Hewlett-Packard's proprietary implementation of the Unix operating system, based on System V (initially System III). It runs on the HP 9000 PA-RISC-based range of processors and HP Integrity Intel's Itanium-based systems.
Decision:	Approved
Decision Constraints:	Products that have been deployed to a production environment may continue to use this technology. All other products must utilize a One-VA TRM approved Linux operating system.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	TRM Team
Vendor Name:	HP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	866: Dependent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Solaris
- AIX
- Red Hat Linux
- Windows (Server)

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date

11i v1	12/1/2000	12/31/2009	12/31/2013
11i v2	9/26/2003	12/31/2010	12/31/2013
11i v3	2/20/2007	12/31/2012	12/31/2017
11i v3.1	9/1/2007	12/31/2012	12/31/2017
11i v3.2	3/1/2008	12/31/2012	12/31/2017
11i v3.3	9/1/2008	12/31/2012	12/31/2017
11i v3.4	4/1/2009	12/31/2012	12/31/2017

VA Forecast Information (09/09/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008				CY2009				CY2010			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
11i v1	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
11i v2	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
11i v3	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
11i v3.1	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
11i v3.2	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
11i v3.3	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**
11i v3.4	None	None	None	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Architectural Area

- Application
- Data
- Integration

Architectural Benefits

- The operating system is a critical component of the VistA infrastructure. Proprietary operating systems such as HP-UX are tightly coupled to the vendor's hardware enabling optimized operation, security and utilization of the enterprise's physical layer components.

Architectural Risks

- Excessive complexity. HP-UX is deployed with other enterprise operating systems in HeV, which include: AIX, RedHat, various Windows server products, and Solaris. This diversity of operating systems significantly complicates server monitoring, application deployment, machine optimization, and capacity planning.

Standards Traceability

- HP publishes extensive standards compliance information for HP-UX 11i v3 at: http://h18004.www1.hp.com/products/quickspecs/12079_div/12079_div.HTML

Tier Used

- Data Tier
- Middle Tier (Infrastructure)
- Middle Tier (Business)
- Middle Tier (Integration)

Tool Type

- Platform

Tool Usage

- Runtime

General Assessment

Expected Usage:	The inclusion of HP-UX in the TRM fulfills the objectives outlined in ENTR68 (now marked as inactive).
Assessment Type:	Refresh
Assessment Date:	9/24/2008
Notes:	

Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Recommend approval as HP-UX is currently implemented in the HeV infrastructure.

2.129) Human Gene Nomenclature (HGN)

General Information

Website:	http://www.genenames.org/cgi-bin/hgnc_stats.pl
Description:	The HUGO Gene Nomenclature Committee (HGNC) aims to assign a unique and ideally meaningful name and symbol to every human gene. The HGNC database currently comprises over 24,000 public records containing approved human gene nomenclature and associated gene information.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	HUGO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (09/09/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**

Forecast Note:	

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.130) HyperText Markup Language (HTML)

General Information

Website:	http://www.w3.org/TR/
Description:	HyperText Markup Language (HTML) is the predominant markup language for web pages. It provides a means to create structured documents by denoting structural semantics for text such as headings, paragraphs, lists etc as well as for links, quotes, and other items. It allows images and objects to be embedded and can be used to create interactive forms.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description

Styles	External Cascading Style Sheets (CSS) are the preferred method for formatting HTML, followed by embedded CSSs, and lastly by embedded HTML

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	886: Static Display

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Cascading Style Sheets (CSS) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.2	1/14/1997		
4.0	12/24/1999		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different

releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
4.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.131) Hypertext Transfer Protocol (HTTP)

General Information

Website: http://tools.ietf.org/html/rfc2817

Description: The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. It is a generic, stateless, protocol which can be used for many tasks beyond its use for hypertext, such as name servers and distributed object management systems, through extension of its request methods, error codes and headers. A feature of HTTP is the typing and negotiation of data representation, allowing systems to be built independently of the data being transferred.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008
Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
HTTP Over TLS	This document describes how to use TLS to secure HTTP connections over the Internet.
Upgrading to TLS Within HTTP/1.1	This document explains how to use the Upgrade mechanism in HTTP/1.1 to initiate Transport Layer Security (TLS) over an existing TCP connection.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- File Transfer Protocol (FTP)

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.1	6/1/1999		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.132) Hypertext Transfer Protocol Services

General Information

Description: Web servers are World Wide Web platforms for creating, managing, and intelligibly distributing informationand on-line applications. The

web server should address Internet message handling, advanced authoring,and a range of security issues. Most web servers enable users to navigate, create, edit, and publish HTML documents in a user-friendly environment. Web servers and application servers allow developers to create arbitrarily complex and highly scalable n-tier applications that can support rapidly growing e-Business needs. They provide Web connectivity, e-Business functionality, runtime services-e.g., load balancing, failover, hot swapping, transaction management, object management, session management, connection pooling - component integration, and application and data integration services.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.133) Identification Authentication

General Information

Description: Identification & Authentication is a set of security measures designed to establish the validity of an identity of a user, user device, or other entity.

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. Currently, authentication is most commonly done through the use of logon passwords. Some business processes may require a more stringent authentication process. The use of digital certificates issued and verified by a Certificate Authority (CA) as part of a Public Key Infrastructure (PKI) is another way to perform authentication with higher assurance. Logically, authentication precedes authorization.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Password Management Policy		VA Information System Account and Password Management Policy (January 2000)

Protection Profiles		VA Security Standards Profile Summary and Department of Veterans Affairs Protection Profiles for Information Systems (November 13, 2001)
Authentication Methods		Authentication methods and technologies implemented by the VA shall offerno less than two-factor authentication.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
NSA - Network Security Guide	The 60 Minute Network Security Guide
NIST FIPS 48	Guidelines On Evaluation Of Techniques For Automated Personal Identification
NIST FIPS 190	Guideline For The Use Of Advanced Authentication Technology Alternatives
NIST SP 800-12	An Introduction to Computer Security: The NIST Handbook
NIST SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
NIST SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
IETF RFC 2989	Criteria for Evaluating AAA Protocols for Network
IETF RFC 3127	Authentication, Authorization, and Accounting: Protocol Evaluation
IETF RFC 3549	Authentication, Authorization and Accounting (AAA) Transport Profile
ISO/IEC 10181-2	Authentication Framework
ASTM E1985	Guide for User Authentication and Authorization
ASTM E1714	Standard Guide for Properties of a Universal Healthcare Identifier (UHID)

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.134) Identification Cards - Integrated Circuit(s) Cards With Contacts

General Information

Website:	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=29257
Description:	ISO/IEC 7816: Identification Cards - Integrated Circuit(s) Cards With Contacts is a standard related to electronic identification cards with contacts, especially smart cards.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Physical characteristics	
Organization, security and commands for interchange	
Interindustry commands for Structured Card Query Language (SCQL)	
Commands for security operations	This document specifies interindustry commands for integrated circuit cards (either with contacts or without contacts) that may be used for ryptographic operations.
Commands for card management	This document specifies interindustry commands for integrated circuit cards (both with contacts and without contacts) for card and file management.
Electronic signals and answer to reset for synchronous cards	This document specifies the power, signal structures, and the structure for the answer to reset between an integrated circuit card(s) with synchronous transmission and an interface device such as a terminal.
Personal verification through biometric methods	This document specifies the usage of interindustry commands and data objects related to personal verification through biometric methods in integrated circuit cards.
Cards with contacts -- USB electrical interface and operating procedures	Tihs document specifies the operating conditions of an integrated circuit card that provides a USB interface. An integrated circuit card with a USB interface is named USB-ICC.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1998			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1998	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.135) ImageGear

General Information

Website:	http://www.accusoft.com/imagegear.htm
Description:	Multi-platform document, medical, and photo imaging SDK that supports over 100 image formats.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v4.1
Decision Date:	10/28/2009
Current Status:	Analysis Completed
Introduced By:	ARB
Vendor Name:	Accusoft Pegasus

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	888: Content Rendering

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
15	11/14/2006		
16	9/26/2008		

VA Forecast Information (09/21/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
15	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
16	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Adoption Benefits

- Mature, stable products
- Supports all approved VA operating systems

Architectural Benefits

- Imaging viewing capability

General Assessment

Expected Usage:	Client imaging viewer for VistA Imaging
Assessment Type:	New
Assessment Date:	9/22/2009
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Accusoft Pegasus is the largest single source provider of imaging software development kits (SDKs) and image viewers, as measured by estimated market share and product offerings. The professional and medical SDKs have been successfully used by VistA Imaging for over 10 years.

2.136) Information Access Privileges to Health Information

General Information

Website:	http://www.astm.org/Standards/E1986.htm
Description:	ASTM E1986: Standard Guide for Information Access Privileges to Health Information covers the process of granting and maintaining access privileges to health information. It directly addresses the maintenance of confidentiality of personal, provider, and organizational data in the healthcare domain. It addresses a wide range of data and data elements not all traditionally defined as healthcare data, but all elemental in the provision of data management, data services, and administrative and clinical healthcare services. In addition, this guide addresses specific requirements for granting access privileges to patient-specific health information during health emergencies.
Decision:	Approved

Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ASTM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
98	1/1/1998		
98(2005)	1/1/2005		
09	1/1/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
98(2005)	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.137) InfoSphere Data Architect

General Information

Website: http://www-01.ibm.com/software/data/studio/data-architect/

Description: InfoSphere Data Architect, formerly known as Rational Data

	Architect, is an Eclipse based enterprise data modeling and integration design tool.
Decision:	Approved
Decision Constraints:	Contact the Software Engineering Tools Management Division for details on the constraints for use of this technology.
Decision Source:	ARB
Decision Process:	TRM v4
Decision Date:	9/16/2009
Current Status:	Analysis Completed
Introduced By:	Enterprise Tools Management
Vendor Name:	IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	870: Modeling

Operating Systems Supported

- Red Hat Linux
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Eclipse - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
7.0	11/28/2006		
7.5	9/26/2008		
7.5.1	12/15/2008		
7.5.2	6/18/2009		

VA Forecast Information (08/14/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
7.5.2	None	None	**Evaluation**	**Planning**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Adoption Benefits

- The use of InfoSphere Data Architect, coupled with available integration to the Rational Software Delivery Platform, increase exposure and oversight of existing data models.

Adoption Risks

- None significant.

Architectural Benefits

- None significant.

Architectural Risks

- None significant.

Tool Usage

- Development
- Modeling/Collaboration

General Assessment

Expected Usage: InfoSphere Data Architect is used for data modeling and integration design.

Assessment Type: New

Assessment Date: 8/18/2009

Notes: InfoSphere Data Architect is an Eclipse based tool, supported under Eclipse v3.4.2, and depends on IBM JDK 1.6 SR5.

InfoSphere Data Architect supports the following data sources:

- Derby v10.x
- Generic JDBC V1.0
- DB2 v8.2, 9.1, 9.5, 9.7
- Informix v10.0, 11.x
- SQL Server 2005
- Oracle v10.x, v11
- MySQL Versions 4.0, 4.1, 5.0, and 5.1
- Sybase Adaptive Server Enterprise Versions 12.0, 12.5, 12.x, 15.0
- Teradata 2.x

InfoSphere Data Architect is 508 compliant.

Recommendation: Approve

Recommendation Constraints:

Recommendation InfoSphere Data Architect is one of several already approved

Justification: IBM modeling tools. It has built-in integrations with the Rational Software Delivery Platform providing lifecycle management and collaboration for data modeling artifacts.

2.138) InstallShield

General Information

Website: http://www.acresso.com/products/installation/installshield.htm

Description: InstallShield is one component of a family of tools that provides the ability to construct installable packages for Windows desktop and server systems. Installable packages can be configured to update application configuration files, executable binaries, data, and registry entries.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: ARB

Decision Process: TRM v2

Decision Date: 9/17/2008

Current Status: Analysis Completed

Introduced By: TRM Team

Vendor Name: Acresso

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	868: Software Configuration Management

Operating Systems Supported

- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
v9	9/23/2003	9/27/2007	9/27/2008
v11	4/1/2005	8/27/2008	8/27/2009
v11.5	10/1/2005	8/27/2008	8/27/2009
v12	5/1/2006		
v2008	8/1/2007		
v2009	6/1/2008		
v2010	6/18/2009		

VA Forecast Information (09/22/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is

considered prohibited from use.

	CY2008				CY2009				CY2010			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
v9	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
v2009	None	None	None	None	Planning	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Architectural Area

- Application

Architectural Benefits

- The deployment and use of a standard installation solution leads to improvements in efficiency and establishes repeatable-consistent practices for HeV personnel.

Architectural Risks

- None significant

EA Requirement

- VA OBJECTIVE E.3 - Implement a One-VA information technology framework that enables the consolidation of IT solutions and the creation of cross-cutting common services to support the integration of information across business lines and provides secure, consistent, reliable, and accurate information to all interested parties.

Tier Used

- Infrastructure Tier

Tool Type

- Tool

Tool Usage

- Management/Collaboration
- Development

General Assessment

Expected Usage:	InstallShield is an install-deployment solution that provides the capability to construct install packages for Windows platforms.
Assessment Type:	Refresh
Assessment Date:	9/22/2008
Notes:	The only known use of InstallShield in the VA is the VIE (Vitria Interface Engine) project.
Recommendation:	Approve
Recommendation Constraints:	None identified
Recommendation Justification:	InstallShield is an off-the-shelf product and has been in use without issue.

2.139) International Classification of Diseases (ICD)

General Information

Website:	http://www.cdc.gov/nchs/icd.htm
Description:	The International Classification of Diseases (ICD) provides codes to classify diseases and a wide variety of signs, symptoms, abnormal findings, complaints, social circumstances and external causes of injury or disease. Every health condition can be assigned to a unique category and given a code. Such categories can include a set of similar diseases.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	N/A

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
ICD-9	1/1/1999		
ICD-9-CM			

ICD-10			
ICD-10-CM			

VA Forecast Information (09/22/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.140) International Nonproprietary Names (INN)

General Information

Website: http://www.who.int/medicines/services/inn/en/index.html

Description: International Nonproprietary Names (INN) facilitate the identification of pharmaceutical substances or active pharmaceutical ingredients. Each INN is a unique name that is globally recognized and is public property. A nonproprietary name is also known as a generic name.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: WHO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Guidance on INN	

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM

technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
58	7/1/2007		
59	1/1/2008		
60	7/1/2008		
61	1/1/2009		
62	7/1/2009		

VA Forecast Information (09/22/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.141) Internet Control Message Protocol (ICMP)

General Information

Website: http://tools.ietf.org/html/rfc792

Description: The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol Suite. It is chiefly used by networked computers' operating systems to send error messages - indicating, for instance, that a requested service is not available or

that a host or router could not be reached.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 792	9/1/1981		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 792	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.142) Internet Explorer

General Information

Website: http://www.microsoft.com/windows/internet-explorer/welcome.aspx

Description:	Internet Explorer is the standard Web browser for HeV (reference VA Directive 6401). Internet Explorer provides access to HeV thin-client applications and Internet-VA intranet sites-applications.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	TRM Team
Vendor Name:	Microsoft

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Access Channels	850: Web Browser

Operating Systems Supported

- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required for some configurations)***
- XSL Transformations (XSLT) - ***(required for some configurations)***

Comparable Technologies/Standards:

- Firefox

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
6.0	8/30/2002	10/1/2006	8/1/2012
7.0	10/1/2006	10/2/2011	10/1/2016
8.0	3/19/2009		

VA Forecast Information (10/16/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
6.0	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
7.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	Field Office IE7 Memo The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment development and deployment using IE is currently based on version 6.

General Analysis

Architectural Area

- Application

Architectural Benefits

- Using a modular browser enables the deployment HeV thin-client applications.

Architectural Risks

- Security issues: as the Web browser market-share leader, Internet Explorer is an attractive target for criminals to exploit security flaws.

EA Requirement

- ENTR 952: VHA shall comply with standards as specified in the VA TRM/SP

Tier Used

- Client Tier
- Presentation Tier (Web)

Tool Type

- Tool

Tool Usage

- Runtime

General Assessment

Expected Usage:	Internet Explorer (IE) provides a standardized deployment and operational platform at the client level in the HeV architecture.
Assessment Type:	Refresh
Assessment Date:	10/2/2008
Notes:	IE 7 had an atypically lengthy development cycle as a result of litigation disputes and extensive product testing. The release of IE 8 is imminent, although no release date has been specified.
Recommendation:	Approve
Recommendation Constraints:	

Recommendation Justification: Recommend approval as Internet Explorer is successfully implemented in the HeV infrastructure.

2.143) Internet Information Services (IIS)

General Information

Website: http://www.iis.net/

Description: Internet Information Services (IIS) - formerly called Internet Information Server - is a set of Internet-based services; FTP, FTPS, SMTP, NNTP, and HTTP/HTTPS for Microsoft Windows based servers

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: ARB

Decision Process: TRM v3.2

Decision Date: 8/19/2009

Current Status: Analysis Completed

Introduced By: TRM Team

Vendor Name: Microsoft

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	871: Web Servers

Operating Systems Supported

- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Windows (Server) - ***(required for some configurations)***
- Windows (Client) - ***(required for some configurations)***

Comparable Technologies/Standards:

- Apache HTTP Server

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5.0	2/17/2000		6/30/2005
6.0	4/23/2003		7/13/2010
7.0	2/4/2008		
7.5	10/22/2009		

VA Forecast Information (10/14/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**

5.0	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
6.0	Evaluation	Evaluation	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
7.0	None	None	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Adoption Benefits

- VA Intranet static and dynamic web content managed by VA Web Operations can continue to be maintained in its current environment
- Mature, well-supported product with high market acceptance

Adoption Risks

- Only available on Windows Server platform

Standards Traceability

- HTTP
- SSL
- FTP
- SMTP

General Assessment

Expected Usage: Manage static and dynamic VA web content

Assessment Type: New

Assessment Date: 6/26/2009

Notes:

Recommendation: Approve

Recommendation Constraints:

Recommendation Justification: IIS is a mature, well supported product with high market acceptance (2nd most popular web server). IIS has been used by VA Web Operations for many years.

2.144) Internet Key Exchange (IKE)

General Information

Website: http://www.rfc-editor.org/rfcsearch.html

Description: The Internet Key Exchange (IKE) is a protocol using part of Oakley and part of Secure Key Exchange Mechnanism (SKEME) in conjunction with Internet Security Association and Key Management Protocol (ISAKMP) to obtain authenticated keying material for use with ISAKMP, and for other security associations such as Authentication Header (AH) and Encapulating Security Payload (ESP) for the IETF IPsec Domain of Interpretation (DOI).

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0 (RFC 2409)	11/1/1998		
2.0 (RFC 4306)	12/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.0 (RFC 2409)	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.145) Internet Message Access Protocol (IMAP)

General Information

Website:	http://tools.ietf.org/html/rfc1734
Description:	Internet Message Access Protocol (IMAP) describes the optional AUTH command, for indicating an authentication mechanism to the server, performing an authentication protocol exchange, and optionally negotiating a protection mechanism for subsequent protocol interactions.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 1734	12/1/1994		
RFC 1939	5/1/1996		
RFC 2449	11/1/1998		
RFC 5034	7/1/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010	CY2011	CY2012

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2449	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.146) Internet Message Format

General Information

Website: http://tools.ietf.org/html/rfc2822

Description: Internet Message Format specifies a syntax for text messages that are sent between computer users, within the framework of "electronic mail" messages.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	871: Web Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2822	4/1/2001		
RFC 4021	3/1/2005		
RFC 5322	10/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the

responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 4021	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.147) Internet Protocol (IP)

General Information

Website: http://tools.ietf.org/html/rfc791

Description: Internet Protocol (IP) provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses. The internet protocol also provides for fragmentation and reassembly of long datagrams, if necessary, for transmission through "small packet" networks.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 791	9/1/1981		

RFC 1349	7/1/1992		
RFC 2474	12/1/1998		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
RFC 791	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.148) Internet Protocol Version 6 (IPv6)

General Information

Website: http://tools.ietf.org/html/rfc2460

Description: Internet Protocol Version 6 (IPv6) Specification is an Internet Layer protocol for packet-switched internetworks. IPv6 is the next-generation Internet Protocol version designated as the successor to IPv4.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM

technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2460	12/1/1998		
RFC 5095	12/1/2007		
RFC 5722	12/1/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2460	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.149) Internet Web

General Information

Description: The Internet is a worldwide system of computer networks in which users at any onecomputer can, if they have permission, get information from any other computer.

Decision: Approved

Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Internet/Intranet Services	VA Directive 6102	This directive defines the organizational responsibilities for all Web activities that govern and/or are related to posting, editing, maintaining, and removing files to or from the Internet and Intranet, the use of emerging Web-based technologies and new uses of existing approved technologies.
Internet/Intranet Services	VA Handbook 6102	This Handbook provides procedures relating to the establishment and administration of a VA Internet and/or Intranet site, and/or site operating on behalf of VA, and/or related service; it also provides procedures for publishing VA information on the World Wide Web (www).

Guidelines and Best Practices

No guidelines have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Delivery Channels	854: Internet

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.150) Intranet Web

General Information

Description:	An Intranet is a private network that is contained within an enterprise. It may consist of many interlinked local area networks and is used to share company information and resources among employees.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Internet/Intranet Services	VA Directive 6102	This directive defines the organizational responsibilities for all Web activities that govern and/or are related to posting, editing, maintaining, and removing files to or from the Internet and Intranet, the use of emerging Web-based technologies and new uses of existing approved technologies.
Internet/Intranet	VA Handbook	This Handbook provides procedures relating to the

Services	6102	establishment and administration of a VA Internet and/or Intranet site, and/or site operating on behalf of VA, and/or related service; it also provides procedures for publishing VA information on the World Wide Web (www).

Guidelines and Best Practices

No guidelines have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Delivery Channels	855: Intranet

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.151) Intrusion Detection and Prevention Systems (IDPS)

General Information

Website: http://csrc.nist.gov/publications/PubsSPs.html

Description: Intrusion Detection Prevention Systems (IDPS) describes the characteristics of IDPS technologies and provides recommendations for designing, implementing, configuring, securing, monitoring, and maintaining them. The types of IDPS technologies are differentiated primarily by the types of events that they monitor and the ways in

which they are deployed.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: NIST

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Security Controls*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
SP 800-31	11/1/2001		2/1/2007
SP 800-94	2/1/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
SP 800-31	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.152) Intrusion Detection Devices

General Information

Description: Intrusion detection services monitor the events occurring in a computer system or network and analyze them for signs of intrusion. An Intrusion Detection System (IDS) is a software or hardware system that automates the process of monitoring the events occurring in a computer system or network, and then analyzing these events forsigns of security problems. Host-Based Intrusion Detection Systems (HIDS) services monitor specific files, logs and registry settings on asingle machine (workstation or server) and can alert on any access, modification, deletion, and copying of the monitored object. The role of a HIDS is to flag any tampering with a specific machine and automatically replace altered files when changed to ensure data integrity. Network-based Intrusion Detection Systems, (NIDS) provide the ability to monitor different segments of the network in order to discover, define and warn about attacks to the network infrastructure.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Placement of IDS	The IDS are not the first line of defense. If firewalls and filtering routers are already in place, thenIDS sensors should be placed inside the network to test the effectiveness of firewall and router policies. Placing sensors inside and outside the firewall provides a pre-emptive capability inidentifying the threat in the early stages of reconnaissance (i.e., scanning and probing).
Use multiple	Whenever possible, IDS deployments should combine products from

products	more than one vendor and more than one type. This gives added assurance that attacks can be detected, since not all the sensors types may be able to detect all the known attacks in any given environment or operating condition.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Security Controls*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.153) IP Authentication Header (AH)

General Information

Website:	http://www.rfc-editor.org/cgi-bin/rfcsearch.pl
Description:	The IP Authentication Header (AH) is used to provide connectionless integrity and data origin authentication for IP datagrams and to provide protection against replays.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA

Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Internet Protocol (IP) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM

technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2402	11/1/1998		
RFC 4302	12/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 4302	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.154) IP Encapsulating Security Payload (ESP)

General Information

Website: http://www.rfc-editor.org/rfcsearch.html

Description: Encapsulating Security Payload (ESP) protocol is designed to provide a mix of security services in IPv4 and IPv6. ESP is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic flow confidentiality.

Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Internet Protocol (IP) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 4303	12/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 4303	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.155) IP Network Address Translator (NAT)

General Information

Website: http://tools.ietf.org/html/rfc2663

Description: Network Address Translation (NAT) is a method by which IP

addresses are mapped from one realm to another, in an attempt to provide transparent routing to hosts. Traditionally, NAT devices are used to connect an isolated address realm with private unregistered addresses to an external realm with globally unique registered addresses. This document attempts to describe the operation of NAT devices and the associated considerations in general, and to define the terminology used to identify various flavors of NAT.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IP Routing Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Internet Protocol (IP) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2663	8/1/1999		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2663	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.156) IP Routing Services

General Information

Description: IP routing services enable packet flow from network to network through routers. The path that a router uses to deliver a packet is defined in its routing table. Routers can statically or dynamically learn the location of traffic destinations from routing protocols. Dynamic routing allows routers to share routing information automatically. If a destination route changes, neighboring routers are informed of the change. The method the router takes to determine a route is described in the specifications of the routing protocol. The routing protocol attempts to find the best path between any source and destination pair in the network. IP routing services provide the capability for routers to find optimum routes, and alternate routes, in the case of network failure or congestion.

Network Address Translation (NAT) performs transparent routing services by performing IP address translation. Transparent routing services are defined as the forwarding of packets from one network to another, and do not require the exchange of routing information. IP address translation is needed when a network's internal IP addresses cannot be used outside the network either because they are private and not valid for use outside, or because the internal addressing must be kept private from the external network. NAT provides the capability to translate public and private addresses in both directions of traffic.

Decision: Approved

Decision Constraints: The Routing Information Protocol (RIP) is not approved for use.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Campus IGP	Campus Interior Gateway Protocols (IGPs) may run another IGP, such as OSPF, within its own campus LAN environment. For design consistency and scalability, it is recommended that the IGP on the LAN be the same as the region WANs.
IP Routing Path	To determine an IP routing path to a remote device, use a middleware operating system utility. The utility may bereferred to as traceroute or tracert, depending on the operating system in use.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.157) IPsec Transport Mode for Dynamic Routing

General Information

Website: http://tools.ietf.org/html/rfc3884

Description: IPsec can secure the links of a multihop network to protect

communication between trusted components, e.g., for a secure virtual network (VN), overlay, or virtual private network (VPN). Virtual links established by IPsec tunnel mode can conflict with routing and forwarding inside VNs because IP routing depends on references to interfaces and next-hop IP addresses. The IPsec tunnel mode specification is ambiguous on this issue, so even compliant implementations cannot be trusted to avoid conflicts. An alternative to tunnel mode uses non-IPsec IPIP encapsulation together with IPsec transport mode, which we call IIPtran. IPIP encapsulation occurs as a separate initial step, as the result of a forwarding lookup of the VN packet. IPsec transport mode processes the resulting (tunneled) IP packet with an SA determined through a security association database (SAD) match on the tunnel header. IIPtran supports dynamic routing inside the VN without changes to the current IPsec architecture. IIPtran demonstrates how to configure any compliant IPsec implementation to avoid the aforementioned conflicts. IIPtran is also compared to several alternative mechanisms for VN routing and their respective impact on IPsec, routing, policy enforcement, and interactions with the Internet Key Exchange (IKE).

Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Internet Protocol (IP) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3884	9/1/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**

RFC 3884	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.158) IPsec-Network Address Translation (NAT)

General Information

Website: http://tools.ietf.org/html/rfc3715

Description: IPsec-Network Address Translation (NAT) Compatibility Requirements describe known incompatibilities between Network Address Translation (NAT) and IPsec, and describe the requirements for addressing them.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Internet Protocol (IP) - Standard
- Network Address Translation - Protocol Translation (NAT-PT) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3715	3/1/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 3715	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.159) IPv6 Client Services

General Information

Description:

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
MPLS	The current process for VPNs with IPv6 is to tunnel over an MPLS IPv4

	backbone. Currently there is no ability to establish an MPLS IPv6 backbone. There is the ability to Overlap IPv6 VPNs through VRF.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.160) IPv6 over Point-to-Point Protocol (PPP)

General Information

Website:	http://tools.ietf.org/html/rfc2472
Description:	IP Version 6 (IPv6) over Point-to-Point Protocol (PPP) defines the method for transmission of IP Version 6 packets over PPP links as well as the Network Control Protocol (NCP) for establishing and configuring the IPv6 over PPP. It also specifies the method of forming IPv6 link-local addresses on PPP links.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA

Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Internet Protocol (IP) - Standard
- Point-to-Point Protocol (PPP) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2472	12/1/1998	9/1/2007	
RFC 5072	9/1/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2472	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.161) IPv6 Performance

General Information

Description: IPv6 performance test should be considered as a first step in creating a baseline, not only for all future IPv6 testing but also to understand any performance differences that may exist in any device that forwards IPv4 and/or IPv6 traffic. These performance tests should not be limited to Quality of Service (QoS), but should

also include Quality of Experience(QoE), to show clear delineation between what is happening on the network, and what the end-user is experiencing.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.162) IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCPv6)

General Information

Website: http://tools.ietf.org/html/rfc3633

Description: The Prefix Delegation options provide a mechanism for automated delegation of IPv6 prefixes using the Dynamic Host Configuration Protocol (DHCP). This mechanism is intended for delegating a long-lived prefix from a delegating router to a requesting router, across an administrative boundary, where the delegating router does not require knowledge about the topology of the links in the network to which the prefixes will be assigned.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Internet Protocol (IP) - Standard
- Dynamic Host Configuration Protocol (DHCP) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3633	12/1/2003		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
RFC	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo

3633	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.163) IPv6/IPv4 Dual Stack Internet Access Service Model

General Information

Website: http://tools.ietf.org/html/rfc4241

Description: IPv6/IPv4 Dual Stack Internet Access Service Model is a digest of the user network interface specification of NTT Communications' dual stack ADSL access service, which provide a IPv6/IPv4 dual stack services to home users. In order to simplify user setup, these services have a mechanism to configure IPv6 specific parameters automatically. The model focuses on two basic parameters: the prefix assigned to the user and the addresses of IPv6 DNS servers, and it specifies a way to deliver these parameters to Customer Premises Equipment (CPE) automatically.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Internet Protocol (IP) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 4241	12/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be

supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 4241	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.164) iText Core

General Information

Website: http://1t3xt.com/products/itext.php

Description: iText Core is the Core framework for dynamic PDF document generation and manipulation. It provides a framework for integrating-building applications requiring automated generation of PDF documents. The iText framework is embedded in a number of products such as Eclipse BIRT and Jasper Reports.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: ARB

Decision Process: TRM v4

Decision Date: 9/16/2009

Current Status: Introduced

Introduced By: Extended Tool List (ETL)

Vendor Name: N/A

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	887: Dynamic Server-Side Display
Component Framework	User Presentation/Interface	888: Content Rendering
Service Interface and Integration	Integration	895: Middleware

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM

technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2.1.0	3/27/2008		
2.1.1	5/1/2008		
2.1.2	5/16/2008		
2.1.3	7/12/2008		
2.1.4	11/11/2008		
2.1.5	3/8/2009		
2.1.6	6/16/2009		
2.1.7	7/7/2009		
2.2.0 (est)	3/1/2010		

VA Forecast Information (08/05/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2.1.6	None	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
2.1.7	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
2.2.0 (est)	None	None	None	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Adoption Benefits

- It would provide an open source framework for implementation of dynamic generation and manipulation of PDF documents within VA Java applications.

- iText is open source allowing for enterprise licensing at no cost to the VA. However it is possible to purchase licenses if required.
- iText is implemented in Java which is skill the VA currently posses and will invest in.
- The ability to dynamically produce and/or manipulate PDF documents and render them in user interface is typically a desired capability in many applications and it improves the user's ability to interface with the system.
- iText has been in use for 9 years and is currently embedded in a number of popular open source reporting tools such as JasperReports and Eclipse BIRT. It is a small embedded framework and its long history indicates maturity which drives operational stability.
- iText is a small framework consisting of a few libraries and from that perspective it is easy to upgrade. However iText is an embedded framework which means that upgrade may impact the enclosing application and can increase the complexity of upgrading or replacing. This will depend on how well the enclosing application abstracts the Technology to allow for easy replacement.

Adoption Risks

- The iText is an open source framework and commercial alternatives from Adobe and other vendors do exist.
- The iText license is held by a California company, but the software is managed by a Belgium company under Belgium law.
- iText support is not well defined and appears to be primarily managed by email and community. Direct support is through 1T3XT BVBA in Belgium and in some case iText Software Corp in California.

Architectural Benefits

- iText is implemented in java which makes it compatible with the to-be architecture.
- iText is implemented in Java making it portable. It will run on all platforms that support the Java Virtual Machine, however portability may be constrained by the enclosing application. This makes iText compatible with current and future infrastructure needs.
- iText is an embedded framework and as such has no IDE integration requirements or restrictions.
- iText is compatible with know 3rd party and VA developed frameworks.
- The iText framework is embedded in popular mainstream open source reporting frameworks such Eclipse BIRT and JasperReports indicating its maturity as an embedded technology.
- Leveraging a framework to dynamically generate and/or manipulate PDF documents will improve delivery speed and reduce costs by eliminating the need to develop and support a custom PDF framework and by providing a consistent approach to incorporating dynamic PDF generation and/or manipulation into VA applications requiring this functionality.

- The iText framework provides a open source Java and .NET framework for dynamically generating PDF documents, which can be embedded into applications requiring the ability to generate and/or manipulate PDF documents directly in the application to support business requirements.

Architectural Risks

- The iText framework is an embedded framework and if not properly abstracted could result in potential lock-in making it difficult to replace in the future should VA needs change.

General Assessment

Expected Usage:	iText will be used to automate the generation of PDF documents and to manipulate existing PDF documents within VA developed applications.
Assessment Type:	New
Assessment Date:	8/7/2009
Notes:	There are additional iText frameworks which are not part of this analysis. This analysis and the recommendation is limited to iText Core. If other iText frameworks are required please request them separately.
Recommendation:	Approve
Recommendation Constraints:	As an embedded technology, it is important to abstract the functionality provided by iText so that it can easily be upgraded or replaced.
Recommendation Justification:	iText met the criteria of a quantitative-qualitative analysis, warranting a recommendation of approval. The only risks identified were risks related to support, which is not well defined and potentially provided by an organization in Belgium. Given the products maturity, targeted use, and lack of alternates in the TRM that covers this functional area--iText is recommended for approval.

2.165) Java AVK

General Information

Website:	http://java.sun.com/j2ee/avk/
Description:	The Java Application Verification Kit (AVK) provides the ability to verify that an application written for the Java platform adheres to Application Program Interface (API) specifications, and will be

portable across compliant platforms.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: ARB

Decision Process: TRM v2

Decision Date: 9/17/2008

Current Status: Analysis Completed

Introduced By: Extended Tool List (ETL)

Vendor Name: Sun Microsystems

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	868: Software Configuration Management

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JDK - Sun Java SE Development Kit - ***(required libraries)***
- WebLogic Server - ***(required for some configurations)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.4.2	2/6/2002		
5.0	9/30/2004		

VA Forecast Information (09/17/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008				CY2009				CY2010			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.4.2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated
5.0	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Architectural Area

- Application
- Data
- Integration

Architectural Benefits

- Supports application portability.
- Use of JAVK promotes adherence to the standards of the Java specifications.

Architectural Risks

- None significant

Standards Traceability

- Java EE - JSF 1.2
- Java EE - Web Service 1.2
- Java EE - EJB 3.0
- Java EE - Servlet 2.5

Tier Used

- N/A

Tool Type

- Tool

Tool Usage

- Development

General Assessment

Expected Usage:	The Java Application Verification Kit (JAVK) will validate adherence of java code to Java Standard Edition (SE) and Java Enterprise Edition (EE) standards.
Assessment Type:	Refresh
Assessment Date:	9/17/2008
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation	This tool provides value by helping to insure that Java

Justification: applications written will port to the various Java EE Application Servers. It also serves to guide developers in the proper use of Java Application Program Interface (API) specifications.

2.166) Java Data Objects (JDO)

General Information

Website: http://java.sun.com/jdo/

Description: The JDO specification provides for interface-based definitions of data stores and transactions; and selection and transformation of persistent storage data into native Java programming language objects.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: Sun Microsystems

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Management	893: Database Connectivity

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Java SE

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	4/30/2002		
2.0	5/1/2006		
2.1	3/17/2008		
2.2	10/24/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010	CY2011	CY2012

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2.1	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
2.2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.167) Java EE

General Information

Website: http://java.sun.com/javaee/index.jsp

Description: The Java Platform, Enterprise Edition, or Java EE (formerly known as J2EE) is a platform for large scale server programming in the Java programming language. Java EE differs from the Standard Edition (SE) of Java in that it adds additional libraries that provide functionality to deploy fault-tolerant, distributed, multi-tier Java software, based largely on modular components running on an application server. It is also a reference implementation of the Java EE specification.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: ARB

Decision Process: TRM v2

Decision Date: 9/17/2008

Current Status: Analysis Completed

Introduced By: Extended Tool List (ETL)

Vendor Name: Sun Microsystems

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Data Types	Char Type, Unsigned Numerical Types, and Enumerations data types should always be avoided because they are not completelydefined in the JAX-RPC and/or XML Schema specification and can lead to unpredictable results. Alternatively, arrays can be used instead of enumerated collections. Complex Data types & Binary Data (via SOAP attachments) should be avoided when JAX-RPC is used to communicate with web services implemented in other languages. Alternatively, binary data can be mapped to xsd:base64Binary and xsd:hexBinary, but this mapping can be inefficient with large amounts of data.

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Java Platform, Enterprise Edition 5 Specification (Java EE 5)	
Implementing Enterprise Web Services	This specification defines the programming model and runtime architecture for implementing web services in Java.
Java API for XML-Based Web Services (JAX-WS)	Added in Java EE 5, JAX-WS is a fundamental technology for developing SOAP based and RESTful Java Web services. JAX-WS is designed to take the place of JAX-RPC in Web services and Web applications.
Java API for XML-Based RPC (JAX-RPC)	Java APIs to support emerging industry XML based RPC standards.
Java Architecture for XML Binding (JAXB)	JAXB provides a convenient way to process XML content using Java objects by binding its XML schema to Java representation.
SOAP with Attachments API for Java (SAAJ)	The SOAP with Attachments API for Java (SAAJ) provides the API for creating and sending SOAP messages by means of the javax.xml.soap package. It is used for the SOAP messaging that goes on behind the scenes in JAX-RPC and JAXR implementations.
Streaming API for XML (StAX) - Added in Java EE 5	The Streaming API for XML (StAX) is a Java based API for pull-parsing XML. StAX provides an alternative to SAX,

	DOM, TrAX, and DOM for developers looking to do high-performance stream filtering, processing, and modification, particularly with low memory and limited extensibility requirements.
Web Service Metadata for the Java Platform	Added in Java EE 5, Web Services Metadata defines an annotated Java format that that uses JavaTM Language Metadata (JSR 175) to enable easy definition of Java Web Services in a J2EE container.
Java Servlet	The Java Servlet specification.
JavaServer Faces - Added in Java EE 5	
JavaServer Pages (JSP)	The JavaServer Pages (JSP) specification.
JavaServer Pages Standard Tag Library (JSTL)	Added in Java EE 5, JSTL is a standard tag library for JSP pages.
Enterprise JavaBeans	The Enterprise JavaBeans specification extends the architecture with integration with JMS, improved support for entity bean persistence, a portable query language for finder methods, support for server interoperability, support for web services, extensions to message-driven beans, enhancements to EJB QL, and a container-managed timer service.
J2EE Connector Architecture (JCA)	The J2EE Connector architecture defines a standard architecture for integrating Java applications with existing back-end Enterprise Information systems.
Common Annotations for the Java Platform	This specification provides annotations for common semantic concepts in the J2SE and J2EE platforms that apply across a variety of individual technologies.
Java Message Service API (JMS)	
Java Persistence API (JPA) - Added in Java EE 5	he Java Persistence API is the Java API for the management of persistence and object/relational mapping for Java EE and Java SE environments.
Java Transaction API (JTA)	Java Transaction API (JTA) specifies standard Java interfaces between a transaction manager and the parties involved in a distributed transaction system: the resource manager, the application server, and the transactional applications.
JavaBeans Activation Framework (JAF)	The JavaBeans Activation Framework specification is a data typing and registry technology that is a Standard Extension to the Java Platform.
JavaMail	The JavaMail API provides a platform-independent and protocol-independent framework to build mail and messaging applications.
J2EE Application Deployment	The J2EE Application Deployment specification provides a

	complete description of the APIs required by the J2EE platform to enable development of platform-independent deployment tools.
J2EE Management	The Java 2 Platform, Enterprise Edition Management Specification will provide server vendors and tool vendors with a standard model for managing the J2EE Platform.
Java Authorization Contract for Containers	This document defines a contract between containers and authorization service providers that will result in the implementation of providers for use by containers
Java Platform 2, Enterprise Edition Specification (J2EE 1.4)	
Java API for XML Parsing (JAXP)	The Java API for XML Parsing (JAXP) allows developers to easily use XML Parsers in their applications via the industry standard SAX and DOM APIs.
Java API for XML Processing	The Java API for XML Processing defines a set of implementation independent portable APIs supporting XML Processing.
Java API for XML Messaging (JAXM)	JAXM provides an API for packaging and transporting business transactions using on-the-wire protocols being defined by ebXML.org, Oasis, W3C and IETF.
Java API for XML Registries (JAXR)	JAXR provides an API for a set of distributed Registry Services that enables business-to-business integration between business enterprises, using the protocols being defined by ebXML.org, Oasis, ISO 11179.
JDBC API	The JDBC API is the industry standard for database-independent connectivity between the Java programming language and a wide range of databases. The JDBC API provides a call-level API for SQL-based database access. JDBC technology allows you to use the Java programming language to exploit "Write Once, Run Anywhere" capabilities for applications that require access to enterprise data.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	887: Dynamic Server-Side Display
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- WebLogic Server - ***(required for some configurations)***

Comparable Technologies/Standards:

- Java SE

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5.0 (aka 1.5)	4/28/2006		
5.2	12/15/2006		
5.3	5/7/2007		
5.4	2/11/2008		
5.5	6/18/2008		

VA Forecast Information (10/14/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
5.2	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**

5.3	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
5.4	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
5.5	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment java development is currently based on Java EE version 5.0.

General Analysis

Architectural Area

- Application
- Data
- Integration

Architectural Benefits

- Java EE provides a standardized, object oriented, application programming language to realize the components of the modular SOA architecture in a platform independent manner.

Architectural Risks

- Performance - applying Java EE to achieve high performance requires both significant programming skill and environmental tuning.
- Complexity - Java EE implementations can achieve excessive numbers of components and resulting system complexities
- Troubleshooting - a Java EE implementation can be designed to leverage capabilities provided by other enterprise components. This can lead to multi-disciplinary troubleshooting of enterprise issues.

Tier Used

- Middle Tier (Infrastructure)
- Client Tier
- Data Tier
- Presentation Tier (Web)
- Middle Tier (Business)
- Middle Tier (Integration)

Tool Type

- Framework

Tool Usage

- Development
- Runtime

General Assessment

Expected Usage:	Java EE is used to create the services, operational, and business logic components of the HeV architecture.
Assessment Type:	Standard
Assessment Date:	9/24/2008
Notes:	Java EE is a Java implementation and a standard, so the technology can be used to deploy functionality and to evaluate Java-based technologies.
Recommendation:	N/A
Recommendation Constraints:	
Recommendation Justification:	

2.168) Java SE

General Information

Website:	http://java.sun.com/javase/index.jsp
Description:	Java Standard Edition (previously known as Java 2 Standard Edition) is the specifications of a java virtual machine and java API (Application Programming Interface). It has been developed under the Java Community Process. JSR 59 was the umbrella specification for J2SE 1.4 and JSR 176 specified J2SE 5.0 (Tiger). Java SE 6 (Mustang) was released under JSR 270. The Java Platform API specification includes: • **User interface Toolkits:** AWT, Swing, Java 2D, Accessibility, Drag n Drop, Input Methods, Image I/O, Print Service, Sound • **Integration Libraries:** IDL, JBDC, JNDI, RMI, RMI-IIOP, Scripting • **Other Base Libraries:** Beans, Intl Support, I/O, JMX, JNI, Math, Networking, Override Mechanism, Security,

Serialization, Extension Mechanism, XML JAXP
- **lang and util Base Libraries:** lang and util, Collections, Concurrency Utilities, JAR, Logging, Management, Preferences API, Ref Objects, Reflection, Regular Expressions, Versioning, Zip, Instrument

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: ARB

Decision Process: TRM v2

Decision Date: 9/17/2008

Current Status: Analysis Completed

Introduced By: Extended Tool List (ETL)

Vendor Name: Sun Microsystems

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Java Language	
Java Virtual Machine	
Java Compiler API	A service provider API that allows a Java program to select and invoke a Java Language Compiler programmatically.
Java Platform, Standard Edition 1.4 (J2SE 1.4)	The Java SE 1.4 specification defines a wide range of general purpose APIs and also includes the Java Language Specification and the Java Virtual Machine Specification. In addition to being used standalone on servers, Java SE is also used as the base for Java Platform, Enterprise Edition ("Java EE").
Java Platform, Standard Edition 5 (Java SE 5)	The Java SE 5.0 specification defines a wide range of general purpose APIs and also includes the Java Language Specification and the Java Virtual Machine Specification. In addition to being used standalone on servers, Java SE is also used as the base for

	Java Platform, Enterprise Edition ("Java EE").
Java Platform, Standard Edition 6 (Java SE 6)	The Java SE 6.0 specification defines a wide range of general purpose APIs and also includes the Java Language Specification and the Java Virtual Machine Specification. In addition to being used standalone on servers, Java SE is also used as the base for Java Platform, Enterprise Edition ("Java EE").
Java API for XML Processing (JAXP)	JAXP defines a set of implementation independent portable APIs supporting XML Processing.
JDBC API	The JDBC API is the industry standard for database-independent connectivity between the Java programming language and a wide range of databases. The JDBC API provides a call-level API for SQL-based database access. JDBC technology allows you to use the Java programming language to exploit "Write Once, Run Anywhere" capabilities for applications that require access to enterprise data.
Java Business Integration (JBI)	This specification extends J2EE and J2SE with business integration SPIs.
Java API for XML-Based Web Services (JAX-WS)	JAX-WS is a fundamental technology for developing SOAP based and RESTful Java Web services. JAX-WS is designed to take the place of JAX-RPC in Web services and Web applications.
Java Architecture for XML Binding (JAXB)	JAXB provides a convenient way to process XML content using Java objects by binding its XML schema to Java representation.
Streaming API for XML (StAX)	Added in Java SE 6, the Streaming API for XML (StAX) is a Java based API for pull-parsing XML. StAX provides an alternative to SAX, DOM, TrAX, and DOM for developers looking to do high-performance stream filtering, processing, and modification, particularly with low memory and limited extensibility requirements.
Web Services Metadata for the Java Platform	This specification defines an annotated Java format that that uses JavaTM Language Metadata (JSR 175) to enable easy definition of Java Web Services in a J2EE container.
XML Digital Signature APIs	This document defines and incorporates a standard set of high-level implementation-independent APIs for XML digital signatures services. The XML Digital Signature specification is defined by the W3C.
Common Annotations for the Java Platform	Added in Java SE 6, this specification provides annotations for common semantic concepts in the J2SE and J2EE platforms that apply across a variety of individual technologies.
Scripting for the Java Platform	Added in Java SE 6, this specification describes mechanisms allowing scripting language programs to access information developed in the Java Platform and allowing scripting language pages to be used in Java Server-side Applications.
Java Management Extensions (JMX)	The JMX specification provides a management architecture, APIs and services for building Web-based, distributed, dynamic and modular solutions to manage Java enabled resources.
Java Naming and	The Java Naming and Directory Interface (JNDI) provides naming

Directory Interface (JNDI)	and directory functionality to applications written in the Java programming language. It is defined to be independent of any specific directory service implementation.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Java EE

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.4.2	2/6/2002		
5 (aka 1.5)	9/30/2004		
6 (aka 1.6)	12/11/2006		

VA Forecast Information (11/23/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.4.2	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
5 (aka 1.5)	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
6 (aka 1.6)	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment development and deployment of Java SE is currently based on version 5.0.

General Analysis

Architectural Area

- Application
- Data
- Integration

Architectural Benefits

- Java is a development language that is independent of the operating system
- Java provides virtual machine approach to platform independence
- Java is standards based
- Java is an object-oriented programming language

Architectural Risks

- A security flaw may be exposed in the Java SE platform; however the possibility is remote considering the excellent security history of the software.

Tier Used

- Middle Tier (Integration)
- Middle Tier (Business)
- Presentation Tier (Thick)
- Client Tier
- Middle Tier (Infrastructure)
- Data Tier

Tool Type

- Platform
- Framework
- Tool

Tool Usage

- Development
- Runtime - Embedded
- Runtime

General Assessment

Expected Usage:	Industry standard object oriented development language and runtime environment.
Assessment Type:	Refresh
Assessment Date:	9/23/2008
Notes:	Approval of this standard does not imply that any reference implementation of this standard is also approved for use.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Java (Java SE) is a foundational platform in the HealtheVet architecture and is essential to the enterprise. Many desktop and browser-based applications depend on the Java SE runtime to function.

2.169) JavaScript

General Information

Website: http://www.ecmascript.org/

Description:	JavaScript is used to write functions that are embedded in or included from HTML pages. For example, programmatically opening a new browser window, validating user input on forms, or to change the appearance of images as the mouse cursor is moved. Because JavaScript code can run locally in a browser (rather than on a remote server) it responds quickly, making an application feel more responsive. A JavaScript interpreter (often referred to as a JavaScript engine) is provided in all of the common Web browsers.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v3
Decision Date:	1/7/2009
Current Status:	Analysis Completed
Introduced By:	TRM Team
Vendor Name:	ECMA

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
ECMAScript Language Specification	This document defines the ECMAScript scripting language.
ECMAScript Compact Profile	This document defines the ECMAScript Compact Profile (ES-CP) scripting language.
ECMAScript for XML (E4X) Specification	This document defines the syntax and semantics of ECMAScript for XML (E4X), a set of programming language extensions adding native XML support to ECMAScript.

FEA Categories

Service Area	Service Category	Service Standard Code

Entry not classified

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Internet Explorer - Standard
- Firefox - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
ECMAScript 1	6/1/1997		
ECMAScript 2	8/1/1998		
ECMAScript 3	12/1/1999		
ECMAScript 4 (est)	12/1/2008		

VA Forecast Information (10/16/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008				CY2009				CY2010			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
ECMAScript 3	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	JavaScript is the colloquial term for vendor-specific implementations of the scripting language that the ECMA body maintains as ECMAScript. Therefore, this forecast is based on the ECMA standard. (Ecma International is a membership-based, non-profit standards organization for information and communication systems).

General Analysis

Architectural Area

- Application

Architectural Benefits

- The browser-based JavaScript interpreter simplifies the deployment model.

Architectural Risks

- Non-standard, vendor-specific implementations of the ECMA language specification.
- JavaScript has the capability to modify resources outside of the browser's run-time environment.

EA Requirement

- ENTR 448: Section 1194.22 Web-based internet information and applications (l)- When pages utilize scripting languages to display content, or to create interface elements, the information provided by the script shall be identified with functional text that can be read by Assistive Technology.
- ENTR 952 - VHA shall comply with standards as specified in the VA TRM/SP

Tier Used

- Client Tier

Tool Type

- Open Source

Tool Usage

- Development

General Assessment

Expected Usage:	For HeV browser-based applications, JavaScript provides client-side programming functionality, (for example, input validation). Client-side programming is desirable as it can eliminate out-of-process, round-trip calls to a remote server, significantly improving performance and the user experience.
Assessment Type:	Standard
Assessment Date:	10/15/2008
Notes:	Note that only Mozilla-based browsers support the unaltered ECMA specification. However, all modern browsers support the ECMAScript specification--up to version 3. JavaScript 1.6-1.9 are code names for the interim versions of ECMAScript that are leading up to JavaScript 2.0 (ECMAScript 4). JavaScript, despite the name, is unrelated to the Java programming language. The language was originally named "LiveScript" but was renamed in a co-marketing deal between Netscape and Sun in exchange for Netscape bundling Sun's Java runtime with their then-dominant browser.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	JavaScript is a standard specified in the Enterprise Architecture TRM/SP.

2.170) JAWS

General Information

Website:	http://www.freedomscientific.com/fs_products/software_jaws.asp
Description:	JAWS for Windows is a software speech synthesizer which uses the computer’s sound card to read aloud information from the screen. JAWS also outputs to refreshable Braille displays, providing Braille support of any screen. This tool is used extensively in HeV for 508 compliance

Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	Freedom Scientific

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Requirements	859: Legislative / Compliance

Operating Systems Supported

- Windows (Client)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
8.0	11/27/2006		
9.0	11/1/2007		
10 (est)			
11 (est)			

VA Forecast Information (09/24/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008				CY2009				CY2010			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
8.0	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
9.0	Planning	Evaluation	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
10 (est)	None	None	None	None	Planning	Evaluation	Supported	Supported	Supported	Supported	Deprecated	Deprecated
11 (est)	None	None	None	None	None	None	None	None	Planning	Evaluation	Supported	Supported
Forecast Note:												

General Analysis

Architectural Benefits

- Architecturally, 508 compliance is a key objective established for all interactive HeV capabilities. The need to make HeV both available and accessible to persons with visual impairments directly serves the HeV community.

Architectural Risks

- None significant

EA Requirement

- ENTR 234 (Inactive) - VHA Goal 1 - Maximize the physical, mental, and social functioning of veterans with disabilities and be recognized as a leader in the provision of specialized health care services. (VA Objective 1.1)
- ENTR 296 - Applications/services shall comply with Section 508 of the Rehabilitation Act of 1973, as amended 29 U.S.C. § 794 (d).

General Assessment

Expected Usage:	Screen readers like JAWS directly support accessibility to individuals with visual impairments and Section 508 compliance objectives.
Assessment Type:	Refresh
Assessment Date:	9/24/2008
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Recommend approval as JAWS is successfully implemented in the HeV and VistA infrastructures.

2.171) JAXB Reference Implementation

General Information

Website:	https://jaxb.dev.java.net
Description:	Provides a reference implementation Java Architecture for XML Binding specification which allows for marshaling and un-marshaling of Java Objects to XML. This implementation is part of Glassfish a reference implementation of the Java Enterprise Edition standards.

	The reference implementation can be used independently in applications requiring the ability to marshal and un-marshal Java Object to XML.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	Sun Microsystems

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- Castor XML
- XMLBeans

Companion Technologies/Standards:

- JAXP Reference Implementation related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0.6	6/26/2006		
2.0.3	10/15/2006		
2.0.5	1/22/2007		
2.1.3	4/13/2007		
2.1.4	7/11/2007		
2.1.5	9/18/2007		
2.1.6	12/19/2007		
2.1.7	5/13/2008		
2.1.8	9/1/2008		

VA Forecast Information (09/26/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008				CY2009				CY2010			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2.0.5	Deprec	Deprec	Deprec	Deprec	Deprec	Deprec	Deprec	Deprec	Deprec	Deprec	Deprec	Deprec

	ated	ated	ated	ated	ated	ated	ated	ated	ated	ated	ated	ated
2.1.5	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment development and deployment of JAXB is currently based on version 2.1.

General Analysis

Architectural Area

- Application
- Data
- Integration

Architectural Benefits

- Supports XML Schema and DTD
- Provides a standards based framework for marshalling/un-marshalling Java Object State to/from XML

Architectural Risks

- Performance: marshaling large XML files may be too slow for some applications.

Standards Traceability

- XML DTD
- Java EE - JAXB 2.0/2.1
- W3C XML Schema

Tier Used

- Middle Tier (Infrastructure)
- Client Tier
- Data Tier
- Presentation Tier (Web)
- Middle Tier (Business)
- Middle Tier (Integration)

Tool Type

- Framework

Tool Usage

- Development
- Runtime - Embedded

General Assessment

Expected Usage:	Marshal-unmarshal XML to-from Java Objects
Assessment Type:	Refresh
Assessment Date:	9/26/2008
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	JAXB is a standards-based reference implementation.

2.172) JAXP Reference Implementation

General Information

Website:	https://jaxp.dev.java.net
Description:	Reference implementation of the Java API for XML Processing (JAXP) specification for parsing, validating, processing, and querying XML documents with Java. The JAXP reference implementation is a part of the Sun Java SDK and is developed as part of the Glassfish project a reference implementation of the Java Enterprise Edition standards. The JAXP specification is a part of the Java Enterprise Edition Standards.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	Sun Microsystems

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- JAXB Reference Implementation related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.3	12/16/2005	2/12/2008	
1.3.1	12/16/2005	2/12/2008	
1.3.2	2/18/2006	2/12/2008	
1.4	10/31/2006		
1.4.1	3/20/2007		
1.4.2	5/30/2007		

VA Forecast Information (09/29/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008				CY2009				CY2010			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.3.2	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
1.4.2	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment development and deployment of JAXP is currently based on version 1.2.

General Analysis

Architectural Area

- Integration
- Application

Standards Traceability

- Java EE - JAXP implements the JAXP 1.3 specification.
- Java EE - JAXP implements the JAXP 1.4 specification.
- JAXP is the reference implementation, implemented as part of JSR-000206 Java

API for XML Processing

Tier Used

- Middle Tier (Infrastructure)
- Client Tier
- Presentation Tier (Web)
- Middle Tier (Business)
- Middle Tier (Integration)

Tool Type

- Framework

Tool Usage

- Development
- Runtime - Embedded

General Assessment

Expected Usage:	To parse, validate and process XML documents within the Java applications.
Assessment Type:	Refresh
Assessment Date:	9/29/2008
Notes:	JAXP refers to both a specification and a reference implementation. In this case this entry is focused on the reference implentation.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	JAXP is a standard component in the Java SE platform. It is the reference implentation of the JAXP specification. It is a mature and stable framework with wide adoption in the industry.

2.173) JPEG

General Information

Website:	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18902

Description:	Specifies processes for converting source image data to compressed image data, processes for converting compressed image data to reconstructed image data, coded representations for compressed image data, and gives guidance on how to implement these processes in practice. Is applicable to continuous-tone - grayscale or color - digital still image data and to a wide range of applications which require use of compressed images. Is not applicable to bi-level image data.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Requirements and guidelines	
Compliance testing	
Extensions	
Registration of JPEG profiles, SPIFF profiles, SPIFF tags, SPIFF colour spaces, APPn markers, SPIFF compression types and Registration Authorities (REGAUT)	

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	888: Content Rendering

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1999	1/1/1999		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010	CY2011	CY2012

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1999	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.174) JPEG 2000

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=37674

Description: JPEG 2000 defines a set of lossless (bit-preserving) and lossy compression methods for coding bi-level, continuous-tone gray-scale, palletized color, or continuous-tone color digital still images.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Core coding system	
Extensions	This document specifies: • extended decoding processes for converting compressed image data to reconstructed image data • an extended codestream syntax • an extended file format • a container to store image metadata • defines a standard set of image metadata • provides guidance on extended encoding processes for converting source image data to compressed image data • provides guidance on how to implement these processes in practice
Motion JPEG 2000	This document specifies the use of the wavelet-based JPEG 2000 codec for the coding and display of timed sequences of images (motion sequences), possibly combined with audio, and composed into an overall presentation. In this specification, a file format is defined, and guidelines for the use of the JPEG 2000 codec for motion sequences are supplied.
Conformance testing	This document specifies the framework, concepts, methodology for testing, and criteria to be achieved to claim compliance with ISO/IEC 15444-1. It provides a framework for specifying abstract test suites and for defining the procedures to be followed during compliance testing.
Compound image file format	This document defines a normative but optional file format for storing compound images using the JPEG 2000 file format family architecture. A compound image is an image that may contain scanned images, synthetic images or both, and that preferably requires a mix of continuous tone and bi-level compression methods. Besides defining a binary container for a mix of continuous-tone and bi-level images, this format defines a composition model that describes how the multiple images are combined to generate a compound image.
Secure JPEG 2000	This document defines: • a normative codestream syntax containing information for interpreting secure image data • a normative process for registering JPSEC tools with a registration authority delivering a unique identifier • informative examples of JPSEC tools in typical use cases • informative guidelines on how to implement security services and

	related metadata
Extensions for three-dimensional data	This document defines a set of lossless (bit-preserving) and lossy compression methods for coding continuous-tone, bi-level, grey-scale, colour digital volumetric images, or multi-component volumetric images. This set of methods extends the elements in the core coding system defined in ISO/IEC 15444-1 and ISO/IEC 15444-2.
Wireless	This document provides a syntax that allows JPEG 2000 coded image data to be protected for transmission over wireless channels and networks. Protection services include error detection and correction capability for header and bitstream, description of the error sensitivity of different portions of the compressed data, and description of possible residual errors in the compressed data. The syntax allows these protection services to be applied to coded image data in part or in their entirety.
ISO base media file format	This document specifies the ISO base media file format, which is a general format forming the basis for a number of other more specific file formats. This format contains the timing, structure, and media information for timed sequences of media data, such as audio/visual presentations.
Interactivity tools, APIs and protocols	This document defines, in an extensible manner, syntaxes and methods for the remote interrogation and optional modification of JPEG 2000 codestreams and files.

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2000	1/1/2000		
2004	1/1/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2004	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.175) JProbe

General Information

Website: http://www.quest.com/jprobe

Description: JProbe analyzes Java code in development environments, looking into the source code to find-report issues affecting performance.

memory, unused code, and test coverage.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: ARB

Decision Process: TRM v2

Decision Date: 9/17/2008

Current Status: Analysis Completed

Introduced By: Extended Tool List (ETL)

Vendor Name: Quest Software

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	869: Test Management

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JDK - Sun Java SE Development Kit - ***(required libraries)***

- Eclipse - ***(required for some configurations)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
7.0.1	7/19/2007		
8.0.1	8/1/2008		
8.1	3/1/2009		
8.2	8/28/2009		

VA Forecast Information (09/09/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008				CY2009				CY2010			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
7.0.1	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
8.0.1	None	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**
8.1	None	None	None	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**
8.2	No	No	No	No	No	No	No	**Planni**	**Evalu**	**Suppo**	**Suppo**	**Suppo**

	ne	ne	ne	ne	ne	ne	ne	ng	ation	rted	rted	rted
Forecast Note:												

General Analysis

Architectural Area

- Application

Architectural Benefits

- JProbe is a tool that can elevate the quality of software, contributing to the architectural goals of a repeatable, consistent development process.

Architectural Risks

- None significant.

Tool Type

- Tool

Tool Usage

- Development
- Runtime

General Assessment

Expected Usage:	Discover, diagnose, and resolve source code problems that impair Java application performance, stability, and scalability.
Assessment Type:	Refresh
Assessment Date:	11/6/2008
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Recommend approval of JProbe as it is successfully implemented in the HeV infrastructure.

2.176) JRules Business Rules Management Server

General Information

Website:	http://www.ilog.com/products/jrules/index.cfm
Description:	JRules is a commercial Java Business Rules Management System (BRMS) providing full lifecycle business rules development, testing, deployment and management of rule-sets integrated into java based applications.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v3.1
Decision Date:	5/13/2009
Current Status:	Introduced
Introduced By:	TRM Team
Vendor Name:	ILOG

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Business Logic	890: Platform Independent Technologies

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***
- WebLogic Server - ***(required for some configurations)***
- Oracle Database - ***(required for some configurations)***
- SQL Server - ***(required for some configurations)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- JRules Rule Execution Server related as: (Suite)
- JRules Scenario Manager related as: (Suite)
- JRules Rule Studio related as: (Suite)
- JRules Team Server related as: (Suite)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
6.5	2/12/2007		
6.6	10/9/2007		
6.7	2/19/2008		

VA Forecast Information (04/24/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009	CY2010	CY2011

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
6.7	None	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	IBM Purchased ILOG in January, 2009, this may impact future versioning and planned releases. Based on past release schedules a new release 6.8 should have been available in February of 2009, but has not been announced. The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment development and deployment of JRules is currently based on version 6.7.1.

General Analysis

Architectural Benefits

- Integration of a Business Rules Management System provides greater flexibility in externalizing frequently changing business rules. This improves agility and allows applications and the business to respond to changes much quicker.
- As the VA moves to Service Oriented Architecture a Business Rules Management System will play a greater role in business process and service orchestration.

Architectural Risks

- ILOG was purchased by IBM in January of 2009. As IBM looks to integrate ILOG JRules into their current products the focus of ILOG JRules will be on Websphere. Though ILOG JRules does support the Java Rules Specification 94 some functionality requires native access. As IBM and ILOG focus on Websphere there may be integration challenges with other J2EE platforms such as WebLogic in the future.
- Though Java Rules Specification 94 provides guidelines for rule administration and rule runtime APIs providing a standard mechanism for integrating 3rd party rules engines, vendors still use proprietary languages to define rules and actions. This results in rule language lock-in not unlike choosing to implement an application in Java or .Net.

Standards Traceability

- JSR-94 Java Rule Engine API Specification

Tier Used

- Middle-Tier (Business)

Tool Type

- Platform

Tool Usage

- Development
- Management/Collaboration
- Runtime

General Assessment

Expected Usage:	To provide a complete business rules management solution that supports the full lifecycle development of business rules that improve VA agility.
Assessment Type:	New
Assessment Date:	4/27/2009
Notes:	The VA may benefit from a more detailed comparative needs analysis of the top modern Business Rules Management Systems such as Blaze, QuickRules and this entry (JRules). Drools which is an open source BRMS has been requested and needs to be addressed
Recommendation:	Approve
Recommendation Constraints:	None identified at this time.
Recommendation Justification:	Currently the VA does not have an approved Business Rules Management System (BRMS). ILOG JRules is one of the most widely used and robust BRMS. With the recent acquisition by IBM it will continue to mature. Approval is recommended for JRules.

2.177) JRules Rule Execution Server

General Information

Website:	http://www.ilog.com/products/jrules/server.cfm
Description:	J2SE/J2EE compliant execution environment for deployment and operation of applications leveraging external business rules.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.

Decision Source:	ARB
Decision Process:	TRM v3.1
Decision Date:	5/13/2009
Current Status:	Introduced
Introduced By:	TRM Team
Vendor Name:	ILOG

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	873: Application Servers

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***
- WebLogic Server - ***(required for some configurations)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- JRules Business Rules Management Server related as: (Suite)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (04/24/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	This tool is part of a suite. Please refer to JRules Business Rules Management Server for the VA Forecast.

General Analysis

General Assessment

Expected Usage:	Part of an overall Business Rules Management System to externalize operational rules from VA software products.
Assessment Type:	New
Assessment Date:	4/27/2009
Notes:	Please refer to the technology entry JRules Business Management System for more information.
Recommendation:	Approve
Recommendation Constraints:	None indentified at this time.

Recommendation Justification:	This technology is part of the JRules Business Rules Management System. As part of the overall solution a server for rules execution is critical. Please refer to the JRules Business Rules Management System for recommendation for more detail.

2.178) JRules Rule Studio

General Information

Website:	http://www.ilog.com/products/jrules/rulestudio.cfm
Description:	An Eclipse-based Integrated Development Environment (IDE) for development of rules based applications. Provides co-editing of rules and java code as well as deployment and debugging of defined rule-sets to the Rule Execution Server. It integrates with the Rule Team Server to provide collaborative development with business rules authors.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v3.1
Decision Date:	5/13/2009
Current Status:	Introduced
Introduced By:	TRM Team
Vendor Name:	ILOG

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	867: Integrated Development Environments (IDE)

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRules Rule Execution Server - ***(required for some configurations)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- JRules Team Server related as: (Companion)
- JRules Business Rules Management Server related as: (Suite)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (04/24/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or

production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	This tool is part of a suite. Please refer to JRules Business Rules Management Server for the VA Forecast.

General Analysis

General Assessment

Expected Usage: To provide an integrated development environment (IDE) to define business rules.

Assessment Type: New

Assessment Date: 4/27/2009

Notes: Please refer to the technology entry JRules Business Management System for more information.

Recommendation: Approve

Recommendation Constraints: None identified at this time.

Recommendation Justification: This technology is part of the JRules Business Rules Management System. As part of the overall solution it is recommended that a integrated development environment (IDE) be included. Though it is possible to develop rules without an IDE, it is not recommended. Please refer to the JRules Business Rules Management System for recommendation for more detail.

2.179) JRules Scenario Manager

General Information

Website: http://www.ilog.com/products/jrules/rsm/index.cfm

Description: Provides rule-set and business simulation unit, regression, functional and impact analysis testing capabilities. Provides facilities for both developer and business user testing.

Decision: Approved

Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v3.1
Decision Date:	5/13/2009
Current Status:	Introduced
Introduced By:	TRM Team
Vendor Name:	ILOG

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	869: Test Management

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRules Rule Execution Server - ***(required for some configurations)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- JRules Business Rules Management Server related as: (Suite)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (04/24/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	This tool is part of a suite. Please refer to JRules Business Rules Management Server for the VA Forecast.

General Analysis

General Assessment

Expected Usage: To test rule-sets implementing in JRules BRMS prior to deployment.

Assessment Type: New

Assessment Date: 4/27/2009

Notes: Please refer to the technology entry JRules Business Management System for more information.

Recommendation: Approve

Recommendation Constraints:	None identified at this time.
Recommendation Justification:	This technology is part of the JRules Business Rules Management System. As part of the overall solution a framework for testing rule-sets and conducting business simulation will provide insure proper rules behavior when deploy to a product environment. Please refer to the JRules Business Rules Management System for recommendation for more detail.

2.180) JRules Team Server

General Information

Website:	http://www.ilog.com/products/jrules/ruleteam.cfm
Description:	Provides a rule repository and management server for authoring, managing, validating and deploying business rules. It is a collaborative environment for rules management.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v3.1
Decision Date:	5/13/2009
Current Status:	Introduced
Introduced By:	TRM Team
Vendor Name:	ILOG

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	868: Software Configuration Management

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- JRules Rule Studio related as: (Companion)
- JRules Business Rules Management Server related as: (Suite)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (04/24/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on

the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	This tool is part of a suite. Please refer to JRules Business Rules Management Server for the VA Forecast.

General Analysis

General Assessment

Expected Usage: To provide a collaborative development environment for defining business rules. Also to provide a repository for storage and versioning of business rules.

Assessment Type: New

Assessment Date: 4/27/2009

Notes: Please refer to the technology entry JRules Business Management System for more information.

Recommendation: Approve

Recommendation Constraints: None identified at this time.

Recommendation Justification: This technology is part of the JRules Business Rules Management System. As part of the overall solution a repository for storage and versioning of rules is important. Business Rules is a collaborative effort and a platform that supports collaboration is highly desirable. JRules Team Server provides both a repository and a collaborative environment for rules development. Please refer to the JRules Business Rules Management System for recommendation for more detail.

2.181) JUnit

General Information

Website: http://www.junit.org

Description:	JUnit is a Java unit test development and testing framework. It provides a framework for developers to rapidly develop and deploy unit tests for their Java development artifacts.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	SourceForge

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	869: Test Management

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.8.2	3/3/2006		
4.0	2/16/2006		
4.1	4/27/2006		
4.2	11/16/2006		
4.3.1	3/28/2007		
4.4	7/18/2007		
4.5	8/8/2008		
4.6	4/14/2009		
4.7	8/4/2009		

VA Forecast Information (09/09/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
3.8.2	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**

4.5	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
4.6	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
4.7	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. The Benefits Segment use of Junit is currently based on version 3.8.1.

General Analysis

Architectural Benefits

- Test Driven Development provides greater application and architectural stability
- A standards based framework for writing and executing java based unit tests

Architectural Risks

- None significant

Tool Type

- Framework
- Tool

Tool Usage

- Development

General Assessment

Expected Usage:	Unit test Java code as part of a test-driven development strategy.
Assessment Type:	Refresh
Assessment Date:	9/26/2008
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Continue use of JUnit.

2.182) Key Management Using ANSI X9.17

General Information

Website: http://csrc.nist.gov/publications/PubsFIPSArch.html

Description: Key Management Using ANSI X9.17 provides cryptographic key management guidance. It consists of three parts. Part 1 provides general guidance and best practices for the management of cryptographic keying material. Part 2 provides guidance on policy and security planning requirements for U.S. government agencies. Finally, Part 3 provides guidance when using the cryptographic features of current systems.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: NIST

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Application-Specific Key Management Guidance	This document provides guidance when using the cryptographic features of current systems.
Best Practices for Key Management Organization	This document provides guidance on policy and security planning requirements for U.S. government agencies.
General	This document provides general guidance and best practices for the management of cryptographic keying material.

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
FIPS 171	4/1/1972	2/8/2005	
SP 800 57	3/1/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be

supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
FIPS 171	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.183) Keyed-Hash Message Authentication Code (HMAC)

General Information

Website: http://csrc.nist.gov/publications/PubsFIPS.html

Description: The Keyed-Hash Message Authentication Code (HMAC) describes a keyed-hash message authentication code (HMAC), a mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative Approved cryptographic hash function, in combination with a shared secret key.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: NIST

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
198	3/1/2002		
198-1	7/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
198	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.184) Layer Two Tunneling Protocol (L2TP)

General Information

Website: http://tools.ietf.org/html/rfc2661

Description: Layer Two Tunneling Protocol (L2TP) specifies multi-protocol access via PPP. L2TP facilitates the tunneling of PPP packets across an intervening network in a way that is as transparent as possible to both end-users and applications.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2661	8/1/1999		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2661	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.185) Lightweight Directory Access Protocol (LDAP)

General Information

Website: http://tools.ietf.org/html/rfc4513

Description: Lightweight Directory Access Protocol (LDAP) describes authentication methods and security mechanisms. It details establishment of Transport Layer Security (TLS) using the StartTLS operation. It also describes the simple Bind authentication method including anonymous, unauthenticated, and name/password mechanisms and the Simple Authentication and Security Layer (SASL) Bind authentication method including the EXTERNAL mechanism.

Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Overview of concepts, models and services	This document introduces the concepts of the Directory and the DIB (Directory Information Base) and overviews the services and capabilities which they provide.
Models	This document provides a number of different models for the Directory as a framework for the other ITU-T Recommendations in the X.500 series. The models are the overall (functional) model, the administrative authority model, generic Directory Information models providing Directory User and Administrative User views on Directory information, generic Directory System Agent (DSA) and DSA information models and operational framework and a security model.
Abstract service definitoin	This document spefines in an abstract way the externally visible service provided by the Directory, including bind and unbind operations, read operations, search operations, modify operations and errors.
Procedures for distributed operations	This document specifies the procedures by which the distributed components of the Directory interwork in order to provide a consistent service to its users.
Protocol specifications	This document specifies the Directory Access Protocol, the Directory System Protocol, the Directory Information Shadowing Protocol and the Directory Operational Binding Management Protocol fulfilling the abstract

	services specified in ITU-T Recommendation X.501 | ISO/IEC 9594-2, ITU-T Recommendation X.511 | ISO/IEC 9594-3, ITU-T Recommendation X.518 | ISO/IEC 9594-4 and ITU-T Recommendation X.525 | ISO/IEC 9594-9. It includes specifications for supporting underlying protocols to reduce the dependency on external specifications.
Selected object classes	This document defines a number of selected object classes and name forms which may be found useful across a range of applications of the Directory. An object class definition specifies the attribute types which are relevant to the objects of that class. A name form definition specifies the attributes to be used in forming names for the objects of a given class.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Active Directory

Companion Technologies/Standards:

- Transport Layer Security (TLS) Protocol - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2830	5/1/2000		
RFC 4513	6/1/2006		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 4513	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Architectural Area

- Application
- Data
- Integration

Architectural Benefits

- LDAP provides a reusable, standardized framework searching hierarchical and organizational data

Architectural Risks

- Support - The current supporting organization provided uncertain support to the protocol and there is no roadmap for future development.
- Proliferation - many vendors have created proprietary implementations of LDAP in their products.

Tier Used

- Client Tier
- Middle Tier (Integration)
- Middle Tier (Infrastructure)
- Data Tier

Tool Type

- Framework

Tool Usage

- Runtime

General Assessment

Expected Usage:	The underlying LDAP standard is currently used in security implementations within the VA.
Assessment Type:	Standard
Assessment Date:	9/30/2008
Notes:	LDAP is a protocol, and this assessment does not describe a specific tool that can be acquired. (There is an open source implementation of LDAP, reference: www.openldap.org). LDAP is a standard consistent with the current architectural direction, can be used both throughout the enterprise and to influence the evaluation of other technologies.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	LDAP is a recognized Internet Protocol standard described in IETF RFC 2251.

2.186) Lightweight EAP (LEAP)

General Information

Website:	
Description:	
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008

Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name:

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.187) Local Area Network (LAN)

General Information

Refer to document: VA_Enterprise_IT_Infrastructure_Standard_LAN_1_0.pdf

Description: This standards document lists the acceptable and recommended specifications for Local Area Network. Sections include standard specifications for subject components, decisions supporting the standard specifications, guidelines or recommendations for implementing the standard specifications, and supplemental factors to consider when evaluating subject components. Other supplementary documents will provide guidance on procuring components that meet the standard specifications, guidance on integrating them with existing components, and explanation of how the subject components fit into the VA Architecture.

This standard includes the following: CORE Network Switch; End-of-Row Access Layer Switch; High-Bandwidth Converged I/O Access Layer Switch; VistA Private SCS DCI Router/Switch; Blade Server Chassis Access Layer Switch; Management Access Layer Switch; Load Balancer.

For each of these standards the following supporting details are included; Chassis, Packet Processor, Linecards/Port Interfaces, Operating System, Support, and High Availability.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EIE CTO

Decision Process: TAR-TAS

Decision Date: 11/5/2009

Current Status: Analysis Completed

Introduced By: OPS/EIE

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	881: Local Area Networks (LAN)

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.188) Log4J

General Information

Website:	http://logging.apache.org/log4j
Description:	Log4J is a Java runtime logging framework that allows developers to include in their source code, the ability to generate logging output messages. The verbosity and output of the log can be controlled by configuration at runtime.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	ASF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	895: Middleware

Operating Systems Supported

- AIX
- HP-UX

- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- JRE - Sun

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.2.14	9/18/2006		
1.2.15	8/24/2007		

VA Forecast Information (10/01/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008				CY2009				CY2010			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.2.1	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**

4												
1.2.15	None	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. The Benefits Segment use of Log4J is currently based on version 1.2.14.

General Analysis

Architectural Area

- Application
- Integration

Architectural Benefits

- Minimizes the use of System.out and other improper logging approaches.
- Provides a standardize mechanism for logging within applications

Architectural Risks

- None significant

Tier Used

- Middle Tier (Infrastructure)

Tool Type

- Framework

Tool Usage

- Development
- Runtime - Embedded

General Assessment

Expected Usage: A standard logging framework for Java applications.

Assessment Type: Refresh

Assessment Date: 9/30/2008

Notes: Log4J is the de-facto standard for Java application logging. Java SE JDK is an alternative, but lags behind Log4J in maturity and robustness. Log4J can work with and is

	complementary to the Enterprise Exception Log Service (EELS).
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Recommend continued use of this tool along with EELS.

2.189) Logical Observation Identifiers Names and Codes (LOINC)

General Information

Website:	http://loinc.org/downloads
Description:	The purpose of LOINC is to facilitate the exchange and pooling of clinical results for clinical care, outcomes management, and research by providing a set of universal codes and names to identify laboratory and other clinical observations.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	LOINC

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Systematized Nomenclature of Medicine-Clinical Terms (SNOMED CT)
- Current Procedural Terminology (CPT)

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2.1	10/31/2003		
2.2	6/30/2007		
2.3	2/26/2010		

VA Forecast Information (10/01/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is

considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. The Benefits Segment use of Log4J is currently based on version 1.2.14.

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.190) Mail Services

General Information

Description:	Mail services pass messages between Message Transfer Agent (MTA) - a program that is responsible for either delivering the message locally or passing it to another MTA, often on another host. MTAs on different hosts on a network often communicateusing SMTP. The message is eventually delivered to the recipient's mailbox - normally a file on his computer - from where he can read it using a mail-reading program (which may or may not be the same Mail User Agent (MUA) as used by the sender).
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Internet/Intranet Services	VA Handbook 6102	This Handbook provides procedures relating to the establishment and administration of a VA Internet and/or Intranet site, and/or site operating on behalf of VA, and/or related service; it also provides procedures for publishing VA information on the World Wide Web (www).

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
IETF RFC 1957	Some Observations on Implementations of the Post Office Protocol (POP3)

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	871: Web Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.191) Malicious Code Detection

General Information

Description:	Malicious Code Detection (anti-virus or virus checking programs) services monitor for viruses and may take action to remove or isolate the virus, preventing it from executing and spreading.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Anti-virus software installation		All PC-based workstations and servers (including those using the Windows, Linux, Unix (all variants), and Macintosh operating systems) shall employ anti-virus software.
Anti-virus software updates		Updated virus detection signatures shall be downloaded and installed at least monthly.
Anti-virus software configuration		Anti-virus software shall be configured to run in a background mode.
Virus scanning		Procedures shall be implemented requiring files to be virus scanned: • incoming to the computer system (e-mail, floppy, CD, FTP, etc.) • before they are attached to outgoing e-mail. A record of the time and date of the scan as well as the tool used should be included in the body of the e-mail. • upon access • on a regularly scheduled basis
Blocking .exe files		Executable files from questionable sources, such as electronic greeting cards and shareware downloads, should be blocked at the external gateways because

		they may contain malicious software.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Technical Cyber Security Alerts	Technical Cyber Security Alerts provide timely information about current security issues, vulnerabilities, and exploits.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Security Controls*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.192) Management Information Base (MIB)

General Information

Website: http://tools.ietf.org/

Description: Management Information Base (MIB) is a type of database used for managing the devices in a communications network. It comprises a collection of objects in a (virtual) database used to manage entities (such as routers and switches) in a network.

Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Structure and Identification of Management Information for TCP/IP-based Internets	This document provides the common definitions for the structure and identification of management information for TCP/IP-based internets.
MIB for TCP/IP	
MIB for SNMP	This document defines managed objects which describe the behavior of a Simple Network Management Protocol (SNMP) entity.
Entity MIB (Version 3)	This document describes managed objects used for managing multiple logical and physical entities managed by a single SNMP agent.
Entity State MIB	This document defines a set of Textual Conventions to represent various states of an entity.
Alarm Management Information Base (MIB)	This document describes management objects used for modelling and storing alarms.
MIB for UDP	This document describes managed objects used for implementations of the User Datagram Protocol (UDP) in an IP version independent manner.
MIB for IP	This document describes managed objects used for implementations of the Internet Protocol (IP) in an IP version

	independent manner.
Remote Network Monitoring MIB	This document defines objects for managing remote network monitoring devices.
MPLS FEC-To-NHLFE MIB	This document describes managed objects for defining, configuring, and monitoring Forwarding Equivalence Class (FEC) to Next Hop Label Forwarding Entry (NHLFE) mappings and corresponding actions for use with Multiprotocol Label Switching (MPLS).
Definitions of Managed Objects for MPLS LDP	This document defines a portion of the Management Information Base (MIB)

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (10/01/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. The Benefits Segment use of Log4J is currently based on version 1.2.14.

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.193) Media Servers

General Information

Description:	Provide optimized management of media based files such as audio and videostreams and digital images.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.194) Medical Device Communications

General Information

Website: http://webstore.ansi.org/FindStandards.aspx?SearchString=1073&SearchOption=0&PageNum=0&SearchTermsArray=null|1073|null

Description: IEEE 1073: The Standard for Medical Device Communications provides a new tool to healthcare providers looking to excel in the new competitive environment. Standardized data communications in life critical acute care situations enables new levels of systems performance for hospital information systems.

Decision: Approved

Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IEEE

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Transport Profile - IrDA Based - Cable Connected	This document defines an IrDA-based transport profile for medical device communications.
Physical Layer Interface - Cable Connected	
Overview and Framework	

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	864: Wireless / Mobile

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1996	1/1/1996		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1996	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.195) Medical Device Interoperability

General Information

Description: Medical Device Interoperability standards allow for health care providers to plug medical or point of care devices into information and computer systems that allows health care providers to monitor information from inpatient bedside or home healthcare environments (a.k.a. Tele-medicine).

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Applicability	Standard for Medical Device Communications (IEEE 1073) should be adhered to when the application is hosted on micro-controller platform, not a PC or server-based platform.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	878: Embedded Technology Devices

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.196) Medical Radiology Images Exchange

General Information

Description:	Medical/Radiology Images Exchange standards facilitate interoperability of diagnostic medical imaging equipment by specifying: (a) A set of protocols to be followed by devices, (b) The syntax and semantics of Commands and associated information, and (c) Information that must be supplied with an implementation.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Clinical Images	DICOM and JPEG-2000 formats should be used to exchange clinical images between imaging systems.
Health Information	HL7 messages should be used to exchange data between imaging systems and health information systems.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.197) Mercury LoadRunner

General Information

Website: http://www.hp.com/go/software

Description: LoadRunner is performance testing software that measures end-to-end response time, diagnoses application and system bottlenecks, and provides the information to enable tuning for better performance. It supports a wide range of enterprise environments

and protocols, including Web Services, Java, and .NET.

Decision: Approved

Decision Constraints: Use of the tool is limited to the SE&I Test Lab and those teams with current licenses.

Decision Source: ARB

Decision Process: TRM v2

Decision Date: 9/17/2008

Current Status: Analysis Completed

Introduced By: Extended Tool List (ETL)

Vendor Name: HP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	869: Test Management

Operating Systems Supported

- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- VuGen related as: (Companion)
- Mercury WinRunner related as: (Companion)
- Mercury Quick Test Professional related as: (Companion)
- Mercury Service Test related as: (Companion)
- Mercury TestDirector related as: (Companion)
- LoadRunner Monitors related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
7.8	9/1/2003		
8.0	8/1/2004		
8.1	10/1/2005		
9.0	8/1/2007		
9.1	2/1/2008		
9.5	9/29/2009		

VA Forecast Information (02/09/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
7.8	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
8.1	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
9.1	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

Forecast Note:	

General Analysis

Architectural Area

- Integration

Tool Type

- Platform

Tool Usage

- Development

General Assessment

Expected Usage:	Provide performance and regression test capability as well as end-to-end performance analysis for systems.
Assessment Type:	Refresh
Assessment Date:	2/10/2009
Notes:	Mercury LoadRunner uses integrated monitors to test against different types of environments. Additional licenses are needed for Web Services monitors for SOAP and XML. No additional licenses are needed to test standard Web servers such as Apache and IIS.
Recommendation:	Approve-Conditional
Recommendation Constraints:	Use of the tool is limited to the SE&I Test Lab and those teams with current licenses.
Recommendation Justification:	Recommend approval of this tool with noted conditions.

2.198) Mercury WinRunner

General Information

Website:	http://www.hp.com/go/software

Description: WinRunner provides functional and regression testing capabilities for application software. WinRunner captures, verifies, and replays user interactions and can generate scripts from those recordings. Recorded scripts can be edited to set up various checkpoints for data integrity and accuracy checking.

Decision: Approved

Decision Constraints: Use of the tool is limited to the SE&I Test Lab and those teams with current licenses.

Decision Source: ARB

Decision Process: TRM v2

Decision Date: 9/17/2008

Current Status: Analysis Completed

Introduced By: Extended Tool List (ETL)

Vendor Name: HP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	869: Test Management

Operating Systems Supported

- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Rational Robot

Companion Technologies/Standards:

- Mercury Business Process Testing related as: (Companion)
- Mercury LoadRunner related as: (Companion)
- Mercury Quick Test Professional related as: (Companion)
- Mercury Service Test related as: (Companion)
- Mercury TestDirector related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
7.5	3/1/2002	7/31/2009	12/31/2010
7.6	1/1/2004	7/31/2009	12/31/2010
8.0	1/1/2005	7/31/2009	12/31/2010
8.2	8/15/2005	7/31/2009	12/31/2010
9.2	3/1/2007	7/31/2009	12/31/2010

VA Forecast Information (01/09/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
7.5	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
7.6	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
9.2	No	**Planni**	**Evalua**	**Suppo**	**Suppo**	**Suppo**	**Suppo**	**Suppo**	**Suppo**	**Suppo**	**Suppo**	**Suppo**

	ne	ng	tion	rted	rted	rted	rted	rted	rted	rted	rted	rted
Forecast Note:												

General Analysis

Architectural Area

- Integration

Tier Used

- Presentation Tier (Thick)

Tool Type

- Platform

Tool Usage

- Development

General Assessment

Expected Usage:	
Assessment Type:	Refresh
Assessment Date:	1/30/2009
Notes:	On February 15, 2008, HP Software announced the end–of–support for HP WinRunner versions 7.5, 7.6, 8.0, 8.2, 9.2—all versions, all editions. WinRunner is being replaced by HP Functional Testing. HP WinRunner customers are entitled to receive an upgrade, under support, which migrates their HP WinRunner license to an equivalent HP Functional Testing 9.5 license upon renewal of their maintenance contract. HP Functional Testing 9.5 includes: HP QuickTest Professional 9.5 + all HP QuickTest Professional 9.5 add-ins + HP WinRunner 9.2.
Recommendation:	Approve-Conditional
Recommendation Constraints:	Use of the tool is limited to the SE&I Test Lab and those teams with current licenses.
Recommendati	Recommend approval as this tool is architecturally relevant to the

on Justification: stated requirements, and it is currently successfully implemented in the HeV infrastructure.

2.199) Messaging Workbench (MWB)

General Information

Website: http://www.hl7.org/special/committees/ictc/docs.cfm

Description: The Messaging Workbench is an HL7 conformance tool that delivers many supporting features. The tool enables development teams to document HL7 messages/profiles that a development team will handle and to test those definitions for consistency with HL7 and local standards.

Messages can be created based upon the library files that represent each version of the HL7 standard, by reverse entry or through manual entry. Additional libraries can be developed for conventions that are implemented locally. The tool includes an MWB diagram bench facilitating a variety of sizeable and configurable shapes to create multiple free form diagrams for each profile. Diagrams can also be imported from other tools that produce BMP or JPG output such as Visio.

A wide array of reports can be generated, printed and exported. The tool can also generate test messages for designed profiles and capture transactions that can be validated against designed profiles. It can also be used to record comments about profiles.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: ARB

Decision Process: TRM v3.2

Decision Date: 8/19/2009

Current Status: Assessment Complete

Introduced By: ARB

Vendor Name: HL7

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	867: Integrated Development Environments (IDE)

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (01/09/2008)

The VA Forecast offers the current and future VA IT position regarding different

releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
Forecast Note:												

General Analysis

Adoption Benefits

- None significant

Adoption Risks

- None significant

Architectural Benefits

- Encourages conformance to the HL7 Standard as the application includes libraries built from the standards for use in developing messages the team will use.

Architectural Risks

- The Messaging Workbench requires a Windows environment.

Standards Traceability

- Microsoft Windows

Tier Used

- Data Tier
- Middleware (Business)

Tool Type

- Application

Tool Usage

- Development
- Management/Collaboration

General Assessment

Expected Usage:	The primary usage is to enable teams to easily and quickly document the structure and details of HL7 messages they will build or parse. It can also be used to a limited degree to generate and receive/validate transactions. Administrative functions enable one to make notes about profiles and to record details associated those profiles.
Assessment Type:	New
Assessment Date:	6/29/2009
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	This tool is being used successfully now and promotes uniformity in profiles submitted to the Message Administrator for approval.

2.200) Metropolitan Area Network Services

General Information

Description:	Metropolitan area network (MAN) services provide access between networks in a metro region.The MAN is the network that picks up traffic from the LAN and passes it to another LAN in the same metro area or to the WAN. The MAN can be described in terms of distance and function. Interms of distance, LANs typically span fewer than two kilometers while MANs can cover distances of up to 150 kilometers. In contrast, the WAN extends beyond the MAN, typically spanning farther than 150 km. In terms of function, a goal of MAN services is to provide secure distributed broadband access to end-users.
Decision:	Approved

Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Fiber Optic Cables		Fiber optic cabling shall be used for connectivity between MANs and LANs

Guidelines and Best Practices

No guidelines have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	Metropolitan Area Network (MAN)*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.201) Mirth Connect

General Information

Website: http://www.mirthcorp.com/products/mirth-connect

Description: Mirth Connect is an open source cross-platform healthcare integration engine that supports the creation of interfaces, or channels, that perform message filtering, transforming, and routing between disparate systems.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: CDCO Supported Architecture Components

Vendor Name: Mirth Corp.

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	896: Enterprise Application Integration

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- BusinessWare
- Mirth Connect

Companion Technologies/Standards:

- Transmission Control Protocol (TCP) related as: (Companion)
- Internet Protocol (IP) related as: (Companion)
- File Transfer Protocol (FTP) related as: (Companion)
- Simple Object Access Protocol (SOAP) related as: (Companion)
- HL7 related as: (Companion)
- XSL Transformations (XSLT) related as: (Companion)
- Digital Imaging and Communications in Medicine (DICOM) related as: (Companion)
- Portable Document Format (PDF) related as: (Companion)
- Rich Text Format (RTF) related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.6	8/16/2006		
1.7	4/25/2008		

1.8	1/15/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.6	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.202) MPEG-1

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=19180

Description: ISO/IEC 11172: Motion Picture Experts Group (MPEG-1) defines a coding standard of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision TRMSP 4.3.2

Process:
Decision Date: 3/14/2008
Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Systems	This document specifies the system layer of the coding. The specification was developed principally to support the combination of the video and audio coding methods defined in ISO/IEC 11172-2 and ISO/IEC 11172-3. The system layer supports the following basic functions: the synchronization of multiple compressed streams on playback, the interleaving of multiple compressed streams into a single stream, the initializiation of buffering for playback start up, continuous buffer management, and time identification.
Video	This document specifies the coded representation of video for digital storage media and the decoding process. It is primarily applicable to digital storage media supporting a continuous transfer rate up to about 1,5 Mbit/s, such as compact disc, digital audio tape, and magnetic hard disc, and for non-interlaced video formats having approximately 288 lines of 352 pels and picture rates around 24 Hz to 30 Hz. Nevertheless it can be used more widely than this because of the generic approach taken.
Audio	This document specifies the coded representation of high quality audio for storage media and the method for decoding of high quality audio signals. Is intended for application to digital storage media providing a total continuous transfer rate of about 1,5 Mbit/s for both audio and video bitstreams, such as CD, DAT and magnetic hard disc, and for sampling rates of 32 kHz, 44,1 kHz, and 48 kHz.
Compliance Testing	This document specifies how tests can be designed to verify whether bitstreams and decoders meet requirements specified in parts 1, 2 and 3 of ISO/IEC 11172. Summarizes the requirements, cross references them to characteristics, and defines how compliance with them can be tested. Gives guidelines how to construct tests and determine their outcome. Defines some actual tests only for audio.

Software simulation	

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1999	11/15/1999		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1999	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.203) MPEG-2

General Information

Website: http://webstore.ansi.org/RecordDetail.aspx?sku=ISO%2fIEC+13818-2%3a2000&source=google&adgroup=iso9&keyword=iso%2Fiec%2013818-2&gclid=CLmYj-zfqaACFdRM5Qod62kycg

Description: ISO/IEC 13818: Motion Picture Experts Group (MPEG-2) Generic coding of moving pictures and associated audio information: Part 2 - Video, specifies the coded representation of picture information for digital storage media and digital video communication and specifies the decoding process.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Systems	This document specifies the systems layer of the coding. The system layer supports six basic functions: • the synchronization of multiple compressed streams on decoding • the interleaving of multiple compressed streams into a single stream • the initialization of buffering for decoding start up • ontinuous buffer management • time identification • multiplexing and signalling of various components in a system stream
Video	
Audio	
Conformance Testing	This document specifies how tests can be designed to verify whether coded data and decoders meet requirements specified in parts 1, 2, 3 and 7 of ISO/IEC 13818.
Software simulation	This document provides a C language software simulation of an encoder and decoder for Part 1 (Systems), Part 2 (Video), Part 3 (Audio), Part 7 (AAC) and Part 11 (IPMP) of ISO/IEC 13818.
Advanced Audio Coding	This document specifies MPEG-2 Advanced Audio Coding (AAC), a multi-channel audio coding standard that delivers higher quality than is achievable when requiring MPEG-1 backwards compatibility. It provides ITU-R "indistinguishable" quality at a data rate of 320 kbit/s for five full-bandwidth channel audio signals.
IPMP on MPEG-2 systems	This document specifies IPMP (Intellectual Property Management and Protection) on the MPEG-2 system. MPEG-2 IPMP offers flexibility, robustness and interoperability, which allows the secure content delivery in the MPEG-2 system. MPEG-2 IPMP can be used in combination with proprietary IPMP tools, which enables the implementation to various degrees of security for different business models, while maintaining the interoperability
Extensions for DSM-CC	
Extensions for	

real time interface for systems decoders	

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2000	12/1/2000		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be

supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2000	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.204) MPEG-4

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38559

Description: ISO/IEC 14496: Motion Picture Experts Group (MPEG-4) specifies system-level functionalities for the communication of interactive audio-visual scenes. It specifies the following:

- a terminal model for time and buffer management
- a coded representation of metadata for the identification, description and logical dependencies of the elementary streams
- a coded representation object content information, a descriptive audio-visual content information
- an interface to intellectual property management and protection systems
- a coded representation of synchronization information
- a multiplexed representation of individual elementary streams in a single stream

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Systems	This document specifies system-level functionalities for the communication of interactive audio-visual scenes.
Visual	The Visual specification contains definitions of the bitstream syntax, bitstream semantics and the related decoding process. It does not specify the encoders, which can be optimized in different implementations.
Audio	This Audio specification integrates many different types of audio coding: natural sound with synthetic sound, low bitrate delivery with high-quality delivery and lossless coding, speech with music, complex soundtracks with simple ones, and traditional content with interactive and virtual-reality content.
Conformance Testing	This document specifies how tests can be designed to verify whether bitstreams and decoders meet requirements specified in parts 1:Systems, 2:Visual, 3:Audio and 6: DMIF. It specifies how tests can be designed for bitstream delivery over various delivery technologies in an interoperable transparent manner.
Delivery Multimedia Integration Framework (DMIF)	This document specifies an interface between the application and the transport, that allows the MPEG-4 application developer to stop worrying about that transport. A single application can run on different transport layers when supported by the right DMIF instantiation.
Reference Software	This document identifies reference software for demonstrating and clarifying the other parts of the standard.
ptimized	This document specifies the encoding tools that enhance both the

reference software for coding of audio-visual objects	execution and quality for the coding of visual objects as defined in Visual
Carriage of ISO/IEC 14496 contents over IP networks	This document provides a framework for the carriage of ISO/IEC 14496 contents over IP networks and guidelines for designing payload format specifications for the detailed mapping of ISO/IEC 14496 content into several IP-based protocols.
Reference hardware description	This document specifies descriptions of the main video coding tools in hardware description language (HDL) form.
Advanced Video Coding	This document pecifies advanced video coding for coding of audio-visual objects.
Scene description and application engine	This document specifies the coded representation of interactive audio-visual scenes and applications.
ISO base media file format	This document specifies the ISO base media file format, which is a general format forming the basis for a number of other more specific file formats. This format contains the timing, structure, and media information for timed sequences of media data, such as audio/visual presentations.
Intellectual Property Management and Protection (IPMP) extensions	This document specifies the definition, as well as Extension tags, syntax and semantics for an IPMP_Data_BaseClass.
MP4 file format	This document specifies the MP4 file format as derived from ISO/IEC 14496-12 and ISO/IEC 15444-12, the ISO base media file format.
dvanced Video Coding (AVC) file format	This document specifies how Advanced Video Coding (AVC) streams are stored in file formats derived from ISO/IEC 14496-12 & 15444-12 (The ISO Base Media File Format).
Animation Framework eXtension (AFX)	This document specifies MPEG-4 Animation Framework eXtension (AFX) model for representing and encoding 3D graphics assets to be used standalone or integrated in interactive multimedia presentations (the latter when combined with other parts of MPEG-4).
Streaming text format	This document specifies a text stream as a concatenation of text access units. A text access unit contains text information of a specific format.
Font compression and streaming	This document defines the set of technologies for compression, encoding and delivery of complex audio-visual scenes composed of different media objects.
ynthesized texture stream	This document specifies the transmission of synthesized texture data as part of the MPEG-4 encoded audio-visual presentation.
Lightweight Application	This document defines a scene description format (LASeR) and an aggregation format (SAF) respectively suitable for representing and

Scene Representation (LASeR) and Simple Aggregation Format (SAF)	delivering rich-media services to resource-constrained devices such as mobile phones.
MPEG-J Graphics Framework eXtensions (GFX)	This document describes a lightweight programmatic environment for advanced interactive multi-media applications. Designed for limited resources devices such as mobile phones.
Open Font Format	This document specifies the Open Font Format (OFF) specification, the TrueType and Compact Font Format (CFF) outline formats, and the TrueType hinting language.
ymbolic Music Representation	This document specifies Symbolic Music Representation (SMR).
Audio and systems interaction	This document describes the desired joint behavior of MPEG-4 Systems (MPEG-4 File Format) and MPEG-4 Audio codecs.
3D Graphics Compression Model	This document describes a model for connecting 3D Graphics Compression tools defined in ISO/IEC 14496 to graphics primitives defined in any other standard, specification or recommendation.
3D Graphics conformance	This document specifies how tests can be designed to verify whether compressed data (i.e. bitstreams) and decoders meet the requirements for the synthetic 3D graphics tools specified in ISO/IEC 14496-11, ISO/IEC 14496-16, ISO/IEC 14496-21, and ISO/IEC 14496-25.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2001			
2004			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2004	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.205) Multimedia Transport

General Information

Description: Multimedia transport services provide a convergence of the existing voice, video, and data infrastructures. Toll bypass applications use routers (gateways) to route voice and fax calls from one telephone switch to another using packet networks instead of the traditional switched telephone network. Transporting voice over a common infrastructure allows the VA to route voice calls between medical centers using the WAN, reducing expenditures on costly leased lines and public network calls and minimizing the operational costs of moving telephone equipment as employees move from location to location. A converged infrastructure will become increasingly important as the VA increases its use of telemedicine and tele-radiology applications.

Decision: Approved

Decision Constraints: PBXs that do not support VoIP capability are not approved for VA use.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
PBX Requirements		New PBX equipment shall support detection and blocking of incoming modem calls where not allowed. This should be done using Caller ID, Time restrictions, and destination phone numbers.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
ITU-T T.121	Data protocols for multimedia conferencing - Generic application template
Toll Bypass Capability	PBXs that do not have toll bypass capability should be replaced or upgraded.
QoS	Switches that do not support QoS should be replaced.
PTSN	PBXs should support PSTN backup.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	Multimedia Transport*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.206) Multiplexing Protocol for Low Bit Rate Multimedia Communication

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=H

Description: ITU-T H.223: Multiplexing Protocol for Low Bit Rate Multimedia Communication specifies a packet-oriented multiplexing protocol for low bit rate multimedia communication. This protocol can be used between two low bit rate multimedia terminals, or between a low bit rate multimedia terminal and a multipoint control unit or an interworking adapter. The protocol allows the transfer of any combination of digital voice/audio, digital video/image and data information over a single communication link. This protocol provides low delay and low overhead by using segmentation and reassembly and by combining information from different logical channels in a single packet.

Decision: Approved

Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2	7/29/2001		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.207) Multipoint Binary File Transfer Protocol

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=T

Description: ITU-T T.127: Multipoint Binary File Transfer Protocol defines a protocol to support the interchange of binary file data within an interactive conferencing or group working environment where the T.120 suite of standards is in use. It provides mechanisms to

support simultaneous distribution of multiple files, selective distribution of files to a subset of participants and retrieval of files from remote sites. Provision is also made for remote directory access.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1	8/11/1995		
2	8/29/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.208) Multipoint Communication Service (MCS) - Service

Definition

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=T

Description: ITU-T T.122: Multipoint Communication Service (MCS) – Service Definition defines a multipoint data delivery service for use in the audiographics and audiovisual conferencing service. It provides the mechanism for multipoint aware applications to send data to all or a subset of the group with a single send primitive and to force, if desired, a uniformly sequenced reception of data at all users. It also provides a token mechanism to allow applications to control scarce resources or do multi-application signalling and synchronization. These services are provided in a manner that is independent of the underlying network connections.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2	2/6/1998		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.209) Multipoint Communication Service (MCS) Protocol

General Information

Website:	http://www.itu.int/itu-t/recommendations/index.aspx?ser=T
Description:	ITU-T T.125: Multipoint Communication Service Protocol Specification defines a protocol operating through the hierarchy of a multipoint communication domain. It specifies the format of protocol messages and procedures governing their exchange over a set of transport connections. The purpose of the protocol is to implement the Multipoint Communication Service defined by ITU-T T.122.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2	2/6/1998		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010	CY2011	CY2012

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.210) Multipoint Control Units for Audiovisual Systems

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=H

Description: ITU-T H.231: Multipoint Control Units for Audiovisual Systems Using Digital Channels up to 1920 kbit/s specifies the means by which three or more audiovisual terminals conforming to Recommendation ITU-T H.320 may communicate simultaneously over constant bit rate digital paths, such communication being designated a "multipoint call".

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3	7/11/1997		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be

supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
3	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.211) Multipoint Still Image and Annotation Protocol

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=T

Description: ITU-T T.126: Multipoint Still Image and Annotation Protocol defines a protocol supporting the management of common multi-layer visual spaces and the multipoint exchange of graphical information directed to these spaces including images (hard and soft copy), pointers, and filled and unfilled parametric drawing elements (points, lines, polygons and ellipses). Support for rendering out-of-band video streams within T.126 workspaces is also included. In addition, keyboard and pointing device exchanges are specified to support basic user interaction. Protocol elements for creating and referencing archived visual spaces are defined to allow pre-stored or pre-distributed graphical materials to be referenced.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Data Protocols for Multimedia Conferencing - Generic Conference Control - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2	7/11/1997		
3	8/29/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.212) Multiprotocol Label Switching (MPLS) Architecture

General Information

Website: http://tools.ietf.org/html/rfc3031

Description: Multiprotocol Label Switching (MPLS) Architecture is a mechanism in high-performance telecommunications networks which directs and carries data from one network node to the next. MPLS makes it easy to create "virtual links" between distant nodes. It can encapsulate packets of various network protocols.

Decision: Approved

Decision No constraints have been specified at this time.

Constraints:	
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
MPLS Management Overview	This document describes the management architecture for MPLS and indicates the interrelationships between the different MIB modules used for MPLS network management.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3031	1/1/2001		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 3031	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.213) Multipurpose Internet Mail Extensions (MIME)

General Information

Website: http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

Description: Multipurpose Internet Mail Extensions (MIME) defines a message representation protocol specifying considerable detail about US-ASCII message headers, and leaves the message content, or message body, as flat US-ASCII text. This set of documents, collectively called the Multipurpose Internet Mail Extensions, or MIME, redefines the format of messages to allow for:

- textual message bodies in character sets other than US-ASCII
- an extensible set of different formats for non-textual message bodies
- multi-part message bodies
- textual header information in character sets other than US-ASCII

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Format of	This document specifies the various headers used to describe the

Internet Message Bodies	structure of MIME messages.
Media Type	This document defines the general structure of the MIME media typing system and defines an initial set of media types.
Message Header Extensions for Non-ASCII Text	This document describes extensions to allow non-US-ASCII text data in Internet mail header fields.
Registration Procedures	This document specifies various IANA registration procedures for the following MIME facilities: media types, external body access types, and content-transfer-encodings.
Conformance Criteria and Examples	This document defines a certain level of implementation that allows the useful interworking of messages with content that differs from US-ASCII text.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2045	11/1/1996		
RFC 2231	11/1/1997		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2045	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.214) MyEclipse

General Information

Website: http://www.myeclipseide.org

Description: MyEclipse is a proprietary release of Eclipse bundled with the most commonly used commercial and open source plug-ins available for Java development (JSE/JEE), WEB, XML and UML. It also integrates Web 2.0/Ajax, Hibernate/Spring, and NetBeans.

Decision: Approved

Decision No constraints have been specified at this time.

Constraints:	
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	Genuitec

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	867: Integrated Development Environments (IDE)

Operating Systems Supported

- Red Hat Linux
- Windows (Client)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***
- Eclipse - ***(required libraries)***
- AJAX - ***(required for some configurations)***

Comparable Technologies/Standards:

- Eclipse

- Rational Software Architect
- Rational Systems Developer

Companion Technologies/Standards:

- Eclipse related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5.1.1	3/1/2007		
5.5	5/1/2007		
6.0	8/1/2007		
6.0.1	10/1/2007		
6.1	3/1/2008		
6.5	6/1/2008		
6.6	10/1/2008		
7 (est)	3/1/2009		

VA Forecast Information (11/10/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008				CY2009				CY2010			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
5.1.1	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
6.0.1	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
6.5	No	No	**Plannin**	**Evaluati**	**Support**	**Suppo**	**Suppo**	**Suppo**	**Depre**	**Depre**	**Depre**	**Depre**

	ne	ne	g	on	ed	rted	rted	rted	cated	cated	cated	cated
7 (est)	None	None	None	None	None	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Architectural Benefits

- Provides a single distribution of Eclipse with the most common commercial and open source plug-ins available in one package; MyEclipse increases developer productivity by reducing the issues associated with manually downloading plug-ins and compatibility issues between plug-ins.

Architectural Risks

- MyEclipse duplicates functionality found in the Rational development tools (RSA, RAD) offered by Enterprise Tools Management. The Rational tools should be utilized unless there is a compelling reason to deviate from the standard.

Tool Type

- Tool

Tool Usage

- Development

General Assessment

Expected Usage:	Provide a single Eclipse-based integrated development environment that includes Eclipse core components and the most common commercial and open source plug-ins.
Assessment Type:	Refresh
Assessment Date:	11/10/2008
Notes:	MyEclipse duplicates functionality found in the Rational development tools (RSA, RAD) offered by Enterprise Tools Management. The Rational tools should be utilized unless there is a compelling reason to deviate from the standard.
Recommendation:	Approve

Recommendation Constraints:	
Recommendation Justification:	Recommend approval for development teams currently productive with MyEclipse. New projects should be using the tool baseline as specified by Enterprise Tools Management.

2.215) Narrow-band Visual Telephone Systems and Terminal Equipment

General Information

Website:	http://www.itu.int/itu-t/recommendations/index.aspx?ser=H
Description:	ITU-T H.320: Narrow-band Visual Telephone Systems and Terminal Equipment specifies technical requirements for narrow-band visual telephone systems and terminal equipment, typically for videoconferencing and videophone services. It describes a generic system configuration consisting of a number of elements which are specified by respective ITU-T Recommendations, definition of communication modes and terminal types, call control arrangements, terminal aspects and interworking requirements.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5	3/15/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
5	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.216) National Cancer Institute Thesaurus (NCIt)

General Information

Website: http://ncit.nci.nih.gov/

Description: NCI Thesaurus (NCIt) provides reference terminology and biomedical ontology for clinical care, translational and basic research, and public information and administrative activities.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: NCI

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Unique Ingredient Identifier (UNII) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is

considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	NCIt is published on a monthly schedule.

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.217) National Drug Code (NDC)

General Information

Website:	http://www.fda.gov/Drugs/InformationOnDrugs/ucm142438.htm
Description:	rug products are identified and reported using a unique, three-segment number, called the National Drug Code (NDC), which is a universal product identifier for human drugs.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	N/A

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is

considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**

VA forecast information is not available for this entry.

Forecast Note:	The NDC Directory is updated on a monthly basis.

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.218) National Drug File – Reference Terminology (NDF-RT)

General Information

Website:	http://evs.nci.nih.gov/ftp1/NDF-RT/
Description:	The National Drug File - Reference Terminology (NDF-RT) is an extension of the VHA National Drug File (NDF). It organizes the drug list into a formal representation. NDF-RT is used for modeling drug characteristics including ingredients, chemical structure, dose form, physiologic effect, mechanism of action, pharmacokinetics, and related diseases.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	N/A

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Unique Ingredient Identifier (UNII) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2009-1	1/13/2009		
2009-2	2/10/2009		
2009-3	3/10/2009		
2009-5	5/12/2009		
2010-1	1/12/2010		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**

VA forecast information is not available for this entry.

Forecast Note:	

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.219) Native Audio Formats

General Information

Description:	The Native Audio formats service deals with the compression, decompression, processing, and encoding representation of audio.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
CD-ROM	Audio burned onto a CD-ROM should be in an MPEG-1 format.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	Native Audio Formats*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.220) Native Document Formats

General Information

Description: Native Document formats are the standard internal organization schemes for human-readable documents meant for public distribution.

Decision: Approved

Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Web Distribution	Documents that are distributed to the general public over the web should be in a PDF format

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	Native Document Formats*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.221) Native Graphics Formats

General Information

Description:	Native Graphics formats are the standard internal organization schemes for static and interactive two- and three-dimensional images.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Thin Client	JPEG is best used for full color “natural” scenes. GIF is best for black & white images or man-made graphics.
Medical	DICOM is the preferred format for medical image exchange.
Vector-based Images	Where applicable, vector-based images should be used as they are scalable without losing detail.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	Native Graphics Formats*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.222) Native Video Formats

General Information

Description:	The Native Video formats service deals with the compression, decompression, processing, and coded representation of combined moving pictures and audio.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
CD-ROM	Video burned onto a CD-ROM should be in an MPEG-2 format.

Streaming (High)	Video broadcasted (streaming) over very high bandwidth devices should be in an MPEG-2 format.
Streaming (Low)	Video broadcasted (streaming) over low bandwidth devices should be in an MPEG-4 format.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	Native Video Formats*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.223) NCPDP Telecommunication Standards

General Information

Website:	http://www.ncpdp.org/standards_purchase.aspx
Description:	This standard addresses the data format and content, the transmission protocol, and other appropriate telecommunication requirements for electronic communication of claims and other transactions between pharmacy providers, insurance carriers, third-party administrators, and other responsible parties.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.

Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	NCPDP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5.0	6/1/1999		
5.1	9/1/1999		
D.0	8/7/2007		
D.2	7/8/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**

VA forecast information is not available for this entry.

Forecast Note:	

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.224) Neighbor Discovery for IPv6

General Information

Website: http://tools.ietf.org/html/rfc2461

Description: Neighbor Discovery for IP Version 6 (IPv6) specifies the Neighbor Discovery protocol for IP Version 6. IPv6 nodes on the same link use

Neighbor Discovery to discover each other's presence, to determine each other's link-layer addresses, to find routers and to maintain reachability information about the paths to active neighbors.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2461	12/1/1998	9/1/2007	
RFC 4311	11/1/2005		
RFC 4861	9/1/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2461	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.225) NetBackup

General Information

Website:	http://www.symantec.com/business/products/family.jsp?familyid=netbackup
Description:	NetBackup provides online backup, and recovery of databases and applications; enables backup and recovery operations over storage networks; and delivers high levels of data security and complete system-level recovery.
Decision:	Approved
Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	Symantec

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- AIX
- HP-UX

- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
6.0	10/1/2005		
6.5	8/1/2007		
7.0	2/1/2010		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

6.5	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.226) Network Address Translation - Protocol Translation (NAT-PT)

General Information

Website:	http://tools.ietf.org/html/rfc2766
Description:	Network Address Translation - Protocol Translation (NAT-PT) specifies an IPv4-to-IPv6 transition mechanism. This solution attempts to provide transparent routing to end-nodes in V6 realm trying to communicate with end-nodes in V4 realm and vice versa.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2766	2/1/2000	7/1/2007	
RFC 4966	7/1/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be

supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2766	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.227) Network Transport

General Information

Description: These consist of the protocols that define the format and structure of data and information that is either accessed from a directory or exchanged through communications.
For the transport of data to take place, each communications process must adhere to rules and procedures. Network protocols are the rules and technical procedures that enable application and middleware communications across the network. In a network, several protocols work together to ensure that the communication is prepared, transferred, received, and acted upon. The work of the Network Protocols must be coordinated so there is no disagreement. To minimize the potential for conflict, protocols operate in layers. Each layer specifies a different function of the communications process. The lower layer protocols specify how vendors can make their equipment connect to other equipment. Middle layer protocols provide session capability for the middleware layer and ensure that the data is able to move reliably between network devices. The upper layer protocols specify rules for application-to-application interaction.
The TCP/IP protocol suite enables transport, file transfer, terminal emulator, messaging, e-mail, and network management capabilities for core infrastructure system services at the middleware and

application layers. The Hypertext TransferProtocol (HTTP), an application level protocol, is the enabler for World Wide Web access.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.228) Network-specific Data Protocol Stacks for Multimedia Conferencing

General Information

Website:	http://www.itu.int/itu-t/recommendations/index.aspx?ser=T
Description:	ITU-T T.123: Network-specific Data Protocol Stacks for Multimedia Conferencing specifies network specific aspects of the T.120-series data protocols for multimedia conferencing. The networks currently identified are ISDN, CSDN, PSDN, PSTN, BISDN, and LAN. Communication profiles are specified which provide reliable point-to-point connections between a terminal and a multipoint control unit, between pairs of terminals or between pairs of MCUs. In some cases, a lower protocol layer allows the multiplexing of audio and video signals in addition to data connections. In other cases, separate calls, over the same or a different network, may be established to carry audio or video signals.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
4	5/27/1999		
5	1/13/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010	CY2011	CY2012

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
4	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.229) Object Linking and Embedding, Database (OLE DB)

General Information

Website: http://msdn.microsoft.com/en-us/library/ms722784%28VS.85%29.aspx

Description: Object Linking and Embedding, Database (OLE DB) is a set of Component Object Model (COM) interfaces that provide applications with uniform access to data stored in diverse information sources and that also provide the ability to implement additional database services. These interfaces support the amount of DBMS functionality appropriate to the data store, enabling it to share its data.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: Microsoft

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Management	893: Database Connectivity

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Open Database Connectivity (ODBC)

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on

the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	See ODBC for forecast information.

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.230) Objects and Attributes for Access Control

General Information

Website:	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18166
Description:	ISO/IEC 10164-9 & ITU-T X.741: Objects and Attributes for Access Control describes an Access Control Security Model and the management information necessary for creating and administering access control associated with OSI System Managements. Security policy adoped for any instance of use is not specified and is left as an implementation choise. This Specification is of generic application and is applicable to the security management of many types of application.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008

Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1995 (1.0)	4/10/1995		
1996 (1.1)	10/5/1996		
1999 (1.2)	6/26/1998		
2002 (1.3)	2/4/2000		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2002 (1.3)	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.231) Office Open XML

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51463

Description: ISO/IEC 29500: Office Open XML defines a set of XML vocabularies for representing word-processing documents, spreadsheets and presentations, based on the Microsoft Office 2008 applications. It

	specifies requirements for Office Open XML consumers and producers that comply to the strict conformance category.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	Native Document Formats*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Portable Document Format (PDF)

- Rich Text Format (RTF)

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2008			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2008	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.232) Open Database Connectivity (ODBC)

General Information

Website: http://msdn.microsoft.com/en-us/library/ms710252%28VS.85%29.aspx

Description: Open Database Connectivity (ODBC) is an application programming interface (API) specification for database access. It is based on the Call-Level Interface (CLI) specifications from Open Group and ISO/IEC for database APIs and uses Structured Query Language (SQL) as its database access language.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: Microsoft

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Management	893: Database Connectivity

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Java SE

Companion Technologies/Standards:

- Object Linking and Embedding, Database (OLE DB) - Standard
- Common Language Infrastructure (CLI) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.5	1/1/1997		
3.8	1/1/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
3.5	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.233) Open Graphics Library (OpenGL)

General Information

Website:	http://www.opengl.org/registry/
Description:	OpenGL (Open Graphics Library) is a standard specification defining a cross-language, cross-platform API for writing applications that produce 2D and 3D computer graphics.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	OpenGL

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2.1	7/2/2006		
3.0	7/11/2008		
3.1	5/28/2009		
3.2	8/3/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
3.0	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo

	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted
3.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.234) Open Shortest Path First (OSPF) Protocol

General Information

Website:	http://tools.ietf.org/html/rfc2328
Description:	Open Shortest Path First (OSPF) Protocol is a specification of the Open Shortest Path First (OSPF) internet routing protocol. OSPF is classified as an Internal Gateway Protocol (IGP).
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IP Routing Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2328	4/1/1998		
RFC 5709	10/1/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2328	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.235) OpenVMS

General Information

Website: http://h71000.www7.hp.com/openvms/operatingsystem.html

Description: OpenVMS is a general-purpose, multi-user operating system. It has well-integrated networking, distributed computing, client/server, multiprocessing, and windowing capabilities.

Decision: Approved

Decision Constraints: Products that have been deployed to a production environment may continue to use this technology. All other products must utilize a One-VA TRM approved Linux operating system.

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: CDCO Supported Architecture Components

Vendor Name: HP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	866: Dependent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
7.3.1	8/1/2002		3/31/2005
8.0	6/1/2003		
8.1	12/1/2003		
8.2	1/1/2005		
8.3	10/1/2007		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
7.3.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.236) Oracle Database

General Information

Website: http://www.oracle.com/database/index.html

Description: The Oracle relational database management system. There are several Oracle editions (Express, Personal, Standard, Enterprise, and Real Application Cluster). This assessment is concerned with the Standard and Enterprise editions of Oracle.

Decision: Approved

Decision Constraints: Benefits Segment development and deployment of Oracle is limited for use only within the Corporate Database

Decision Source: ARB

Decision Process: TRM v2

Decision Date: 9/17/2008

Current Status: Analysis Completed
Introduced By: Extended Tool List (ETL)
Vendor Name: Oracle

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Database/Storage	875: Database

Operating Systems Supported

- AIX
- HP-UX
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Structured Query Language (SQL) - ***(required for some configurations)***

Comparable Technologies/Standards:

- Cache Database Engine
- SQL Server

Companion Technologies/Standards:

- Oracle JDBC Drivers related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
8.1	4/1/1999		
9.2	3/1/2002		
10.1	5/1/2004		
10.2	5/1/2005		
11.1	5/1/2007		
11.2	9/1/2009		

VA Forecast Information (04/09/2010)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
8.1	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
9.2	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
10.2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
11.1	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment development and deployment of Oracle Database is currently based on version 10.2.

General Analysis

Architectural Area

- Data

EA Requirement

- ENTR 1074 - Implement a One VA information technology framework that supports the integration of information across business lines and that provides a source of consistent, reliable, accurate, and secure information to veterans and their families, employees, and stakeholders (Enabling Objective E-3).
- ENTR 239 - VA Enabling Goal - Deliver World-Class Service: Deliver world-class service to veterans and their families by applying sound business principles that result in effective management of people, communications, technology, and governance.

Standards Traceability

- ANSI SQL 92

Tier Used

- Data Tier

Tool Type

- Framework
- Tool
- Platform

Tool Usage

- Development
- Management/Collaboration
- Runtime

General Assessment

Expected Usage:	Provide an enterprise class commercial relational database management system with the ability to store and retrieve veterans' information securely and reliably.
Assessment Type:	Refresh
Assessment Date:	9/18/2008
Notes:	
Recommendation:	Approve
Recommendati	

on Constraints:	
Recommendation Justification:	Continue using Oracle as the production database.

2.237) Oracle JDBC Drivers

General Information

Website:	http://www.oracle.com/technology/tech/java/sqlj_jdbc/index.html
Description:	Java DataBase Connect (JDBC) is the industry standard for database-independent connections between the Java programming language and a wide range of databases. A vendor-neutral JDBC driver can be used through Open Data Base Connectivity (ODBC) but this causes performance and functionality to suffer. The best application performance on an Oracle database is attained with specialized Oracle JDBC drivers. The Oracle Thin Driver is best for HeV applications.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	Oracle

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Management	893: Database Connectivity

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- Cache JDBC Driver

Companion Technologies/Standards:

- Java SE related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
9.2	3/1/2002		
10.1	5/1/2004		
10.2	2/1/2006		
11.1	5/1/2007		

VA Forecast Information (09/25/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008				CY2009				CY2010			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
9.2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Deprecated	Deprecated
10.2	None	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
11.1	None	None	None	None	None	None	None	None	Planning	Evaluation	Supported	Supported
Forecast Note:												

General Analysis

Architectural Benefits

- Common technologies support standardized skills, realization of best practices, and improvements in developer efficiency.

Architectural Risks

- Complexity - Oracle produces 4 major variants of its JDBC driver for specialized applications. The Oracle Thin Driver is optimal for the HeV environment.

Standards Traceability

- SQL

General Assessment

Expected Usage:	Developer productivity and work product quality are directly enhanced by the use of a standardized database connectivity approach. Oracle JDBC supports this objective.
Assessment Type:	Refresh
Assessment	9/25/2008

Date:	
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Recommend approval as the Oracle JDBC Drivers are successfully implemented in the HeV infrastructure.

2.238) Packet-Based Multimedia Communications Systems

General Information

Website:	http://www.itu.int/itu-t/recommendations/index.aspx?ser=H
Description:	ITU-T H.323: Packet-Based Multimedia Communications Systems describes terminals and other entities that provide multimedia communications services over Packet-Based Networks (PBN) which may not provide a guaranteed Quality of Service. H.323 entities may provide real-time audio, video and/or data communications. Support for audio is mandatory, while data and video are optional, but if supported, the ability to use a specified common mode of operation is required, so that all terminals supporting that media type can interwork.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
6	6/13/2006		
7	12/14/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different

releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
6	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.239) Parallel Sysplex

General Information

Website: http://www-03.ibm.com/systems/z/advantages/pso/index.html

Description: Parallel Sysplex is a clustering technology. It allows IBM mainframes to act together as a single system image with z/OS. Used for disaster recovery, Parallel Sysplex combines data sharing and parallel computing to allow a cluster of up to 32 systems to share a workload for high performance and high availability.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: CDCO Supported Architecture Components

Vendor Name: IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	866: Dependent Platform

Operating Systems Supported

- z/OS

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Oracle RAC

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date

Vendor release information is not available for this entry.

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	See z/OS for release and VA Forecast information

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.240) Password Services

General Information

Description: A password is a protected and private string of numbers, text, and other characters used to authenticate an identity.

A password is an un-spaced sequence of characters used to determine that a computer user requesting access to a computer system is really that particular user. Typically, users of a multi-user or securely protected single-user system claim a unique name (often called a userID) that can be generally known. In order to authenticate that someone entering that user ID really is that person, a second identification, the password, known only to that person and to the system itself, is entered by the user.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Password Management Policy		VA Information System Account and Password Management Policy (January 2000)

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
NSA - Network Security Guide	The 60 Minute Network Security Guide
NIST FIPS 48	Guidelines On Evaluation Of Techniques For Automated Personal Identification
NIST FIPS 112	Password Usage
NIST FIPS 181	Automated Password Generator (APG)
NIST FIPS 190	Guideline For The Use Of Advanced Authentication Technology Alternatives
NIST SP 800-12	An Introduction to Computer Security: The NIST Handbook
NIST SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
NIST SP 800-23	Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.241) Performance Management

General Information

Description:	Performance management measures available performance parameters to ensure that acceptable levels of performance are maintained. Performance management strives to achieve network conditions where users are satisfied in terms of network responsiveness. Performance management evaluates and reports on the behavior of telecommunications equipment and the effectiveness of the network or network devices. End-to-end performance management measures performance across an internetwork. Component performance measures the performance of individual links or devices. Performance management gathers statistical information, maintains and examines historical logs, determines system performance under natural and simulated conditions.To ensure that the VA is receiving a maximum return on its technical investment, service level agreements (SLAs) should be obtained to confirm that the performance is at the expected levels.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision	TRMSP 4.3.2

Process:
Decision Date: 3/14/2008
Current Status: Analysis Completed
Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Network Management		The network management system shall display management data, monitor and control managed devices, and communicate with management agents. Data link and physical layer parameters shall be monitored by management systems that are based on Management Information Base (MIB) - Remote Monitoring (RMON) standards.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Management Device	A router, server, switch, or end system should be selected on each network to be a local management device.
Problem Notification	Users should be informed about ongoing problems, and given a timeframe for resolution.
Problem Resolution Documentation	After a problem is resolved, the problem/resolution should be tested and then documented in a problem-tracking database.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	Network Management Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.242) Person Identification Service (PIDS)

General Information

Website:	http://www.omg.org/technology/documents/formal/person_identification_service.htm
Description:	This specification defines the interfaces of a CORBA Person Identification Service (PIDS) that organizes person ID management functionality to meet healthcare needs.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	OMG

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.1	4/4/2001		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010	CY2011	CY2012

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.243) Pharmacological Orders Exchange

General Information

Description: Pharmacological Orders Exchange standards allow pharmacies to standardize information between health care providers and the pharmacies for ordering drugs and to facilitate electronic submission of pharmacy claims at the point of service.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.244) PlateSpin Migrate

General Information

Website:	http://www.novell.com/products/migrate/
Description:	PlateSpin Migrate is a workload portability solution that automates the movement of server workloads - operating systems along with their applications and data - over the network between physical servers, virtual hosts and image archives. PlateSpin Migrate remotely decouples workloads from the underlying server hardware and streams them to and from physical or virtual hosts, all from a single point of control.
Decision:	Approved
Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009

Decision Date: 6/15/2009
Current Status: Analysis Completed
Introduced By: CDCO Supported Architecture Components
Vendor Name: Novell

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	Network Management Services*

Operating Systems Supported

- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM

technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
8.1	7/24/2008		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
8.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.245) PlateSpin PowerConvert

General Information

Website: http://www.platespin.com/products/powerconvert/

Description: PowerConvert is a workload portability and protection solution that optimizes the data center by streaming server workloads over the network between physical servers, virtual hosts and image archives. PowerConvert remotely decouples workloads from the underlying server hardware and streams them to and from any physical or virtual host.

Decision:	Approved
Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	Novell

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	Network Management Services*

Operating Systems Supported

- Red Hat Linux
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Internet Information Services (IIS) - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
6.6	5/15/2007		
7.0	6/24/2008		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
7.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.246) PlateSpin Protect

General Information

Website: http://www.novell.com/products/protect/

Description: PlateSpin Protect is a workload protection solution that replicates and rapidly recovers server workloads - operating systems along with their applications and data - all from a single point of control. In the event of a production server outage or disaster, workloads can be rapidly powered on and continue to run as normal until the production environment is restored. PlateSpin Protect provides a simple, flexible and cost-effective solution for protecting physical and virtual workloads in the data center.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: CDCO Supported Architecture Components

Vendor Name: Novell

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	Network Management Services*

Operating Systems Supported

- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
8.0	12/6/2008		
8.1	7/25/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
8.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.247) Point-of-care Medical Device Communication

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=36347

Description: ISO/IEEE 11073: Point-of-care Medical Device Communication is a family of standards addressing the interoperability of medical devices. The ISO/IEEE 11073 standard family defines parts of a system, with which it is possible, to exchange and evaluate vital signs data between different medical devices, as well as remote control these devices.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Nomenclature	This document covers nomenclature architecture for point-of-care (POC)

	medical device communication (MDC).
Application profiles - Base standard	This document provides the upper layer [i.e., the International Organization for Standardization's (ISO's) open systems interconnection (OSI) application, presentation layer, and session layer] services and protocols for information exchange.
Transport profile - Cable connected	This document describes an IrDA-based, cable-connected local area network (LAN) for the interconnection of computers and medical devices and is suitable for new device designs, but is particularly targeted to modifications of legacy devices.
Transport profile - Infrared wireless	This document efines an IrDA-based transport profile for medical device communication that uses short-range infrared, as a companion standard to ISO/IEEE 11073-30200, which specifies a cable-connected physical layer.
Analytical instruments - Point-of-care test	This document establishes a set of specifications to allow seamless multivendor interoperability and communication between point-of-care devices, data concentrators, and clinical information systems.
Computer-assisted electrocardiography	This document specifies the common conventions required for the cart-to-host as well as cart-to-cart interchange of specific patient data (demographic, recording, ...), ECG signal data, ECG measurement and ECG interpretation results.
Encoding rules	This document specifies how medical waveforms, such as electrocardiogram, electroencephalogram, spirometry waveform etc., are described for interoperability among healthcare information systems.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	878: Embedded Technology Devices

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2004	1/1/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2004	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.248) Point-to-Point Protocol (PPP)

General Information

Website: http://tools.ietf.org/html/rfc2153

Description: Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. PPP defines an extensible Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection; and a family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2153	5/1/1997		
RFC 5342	9/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2153	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.249) Portable Document Format (PDF)

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51502

Description: ISO 32000-1: Portable Document Format (PDF) specifies a digital form for representing electronic documents to enable users to exchange and view electronic documents independent of the environment in which they were created or the environment in which they are viewed or printed.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	Native Document Formats*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Rich Text Format (RTF)
- Office Open XML

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2008 (aka PDF 1.7)	7/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2008 (aka PDF 1.7)	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.250) Portable Network Graphics (PNG)

General Information

Website:	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=29581
Description:	Portable Network Graphics (PNG, pronounced "ping") specifies a datastream and an associated file format, for a lossless, portable, compressed individual computer graphics image transmitted across the Internet. Indexed-colour, greyscale, and truecolour images are supported, with optional transparency. Sample depths range from 1 to 16 bits. PNG is fully streamable with a progressive display option.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2003	11/10/2003		
2004	3/3/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2004	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.251) Portlet

General Information

Website: http://www.jcp.org/en/jsr/all

Description: To enable interoperability between Portlets and Portals, this specification defines a set of APIs for Portal computing addressing the areas of aggregation, personalization, presentation and security.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: Sun Microsystems

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Portlet specification 1.0	
Portlet specification 2.0	
Portlet Bridge Specification for JavaServer Faces	The Portlet Bridge Specification for JavaServer Faces defines the semantics of a JSR 168/JSR 286 portlet that proxies for JSF artifacts.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	10/27/2003		
2.0	6/12/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.252) Post Office Protocol (POP)

General Information

Website: http://tools.ietf.org/html/rfc2449

Description: Post Office Protocol (POP) is an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2449	11/1/1998		
RFC 5034	7/1/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2449	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.253) PPP Triple-DES Encryption Protocol (3DESE)

General Information

Website: http://www.rfc-editor.org/rfcsearch.html

Description: The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links.

The PPP Encryption Control Protocol (ECP) provides a method to negotiate and utilize encryption protocols over PPP encapsulated links.

This document provides specific details for the use of the Triple-DES standard (3DES) for encrypting PPP encapsulated packets.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2420	9/1/1998		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2420	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.254) Primavera TeamPlay

General Information

Website: http://www.oracle.com/primavera/index.html

Description: Primavera TeamPlay is an integrated multi-project management solution that combines workgroup/project team communications, integrated methodology/process management, enterprise wide project tracking, and integrated risk and issue management with core project management functions.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: HSD&D

Decision Process: ETL

Decision Date: 12/1/2006

Current Status: Introduced

Introduced By: Extended Tool List (ETL)

Vendor Name: Oracle

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
N/A	N/A	N/A

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

ETL Approved Technology/Standard, TRM Analysis still pending.

General Assessment

ETL Approved Technology/Standard, TRM Assessment still pending.

2.255) Processor Area Network (PAN) Manager

General Information

Website: http://www.egenera.com/products-panmanager-ex.htm

Description: Processor Area Network (PAN) Manager aggregates and abstracts industry-standard x86 servers, I/O, SAN storage and data networks into agile resource pools, enabling those resources to be rapidly and automatically re-allocated based upon business requirements.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: CDCO Supported Architecture Components

Vendor Name: Egenera

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5.2	1/20/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
5.2	Evalua	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo

	tion	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.256) Protected Extensible Authentication Protocol (PEAP)

General Information

Website: http://googleads.sgdoubleclick.net/pagead/nclk?sa=L&ai=1&fadurl=googleads.g.doubleclick.net&u=http%3A%2F%2Fdownload.microsoft.com%2Fdownload%2F9%2F5%2FE%2F95EF66AF-9026-4BB0-A41D-A4F81802D92C%2F%255BMS-PEAP%255D.pdf&aclck=http%3A%2F%2Fbabythought.com%2Findex.php

Description: Protected Extensible Authentication Protocol (PEAP) is a part of the family of Extensible Authentication Protocol (EAP) protocols. PEAP uses Transport Level Security (TLS) to create an encrypted channel between an authenticating PEAP client, such as a wireless computer, and a PEAP authenticator, such as an Internet Authentication Service (IAS) or Remote Authentication Dial-In User Service (RADIUS) server. PEAP does not specify an authentication method, but provides additional security for other EAP authentication protocols, such as EAP-MSCHAPv2, that can operate through the TLS encrypted channel provided by PEAP. PEAP is used as an authentication method for 802.11 wireless client computers, but is not supported for virtual private network (VPN) or other remote access clients.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: Microsoft

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Transport Layer Security (TLS) Protocol - Standard
- Remote Authentication Dial In User Service (RADIUS) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
v0/EAP-MSCHAPv2			
v1/EAP-GTC			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
v0/EAP-MSCHAPv2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.257) Public Key Infrastructure

General Information

Description: The Public Key Infrastructure (PKI) is a framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies.

PKI provides for a digital certificate that can identify an individual or

an organization and directory services that canstore and, when necessary, revoke the certificates. PKI facilitates the use of public key cryptography, which is acommon method for authenticating an individual or encrypting a file. PKI consists of:

- A certificate authority (CA) issues and verifies digital certificate. A certificate includes the public key orinformation about the public key
- A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate isissued to a requestor
- One or more directories where the certificates (with their public keys) are held
- A certificate management system

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Federal Bridge Certificate Authority (FBCA) Certificate Policy		X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)
VA PKI Certificate Policy		Department of Veterans Affairs, VA PKI: Certificate Policy, DRAFT v2.0, June 14, 1999

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description

NIST FIPS 48	Guidelines On Evaluation Of Techniques For Automated Personal Identification
NIST FIPS 190	Guideline For The Use Of Advanced Authentication Technology Alternatives
NIST FIPS 196	Entity Authentication Using Public Key Cryptography
NIST SP 800-2	Public-Key Cryptography
NIST SP 800-15	Minimum Interoperability Specification for PKI Components (MISPC), Version 1
NIST SP 800-21	Guideline for Implementing Cryptography in the Federal Government
NIST SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
NIST SP 800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure
IETF RFC 3447	PKCS #1-RSA Cryptography Standard: RSA Cryptography Specifications V2.1
IETF RFC 2315	PKCS #7-Cryptographic Message Syntax v1.5
IETF RFC 2527	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
IETF RFC 2631	PKCS #3-Diffie-Hellman Key Agreement Method
IETF RFC 2985	PKCS #9-Selected Object Classes and Attribute Types v2.0
IETF RFC 2986	PKCS #10-Certification Request Syntax Specificatio v1.7
PKCS #6	PKCS #6-Extended-Certificate Syntax Standard
PKCS #8	PKCS #8-Private-Key Information Syntax Standard
PKCS #11	PKCS #11-Cryptographic Token Interface Standard
PKCS #12	PKCS #12-Personal Information Exchange Syntax Standard
PKCS #13	PKCS #13-Elliptic Curve Cryptography Standard
ASTM E2212-02	Standard Practice for Healthcare Certificate Policy

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.258) Pulse Code Modulation (PCM) of Voice Frequencies

General Information

Website:	http://www.itu.int/itu-t/recommendations/index.aspx?ser=G
Description:	ITU-T G.711: Pulse Code Modulation (PCM) of Voice Frequencies defines the characteristics for encoding voice-frequency signals.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5	11/15/1988		
5.1	9/30/1999		
5.2	2/12/2000		
5.3	8/29/2009		
5.4	11/6/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
5.2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.259) Radio Frequency Management

General Information

Description: Radio Frequency (RF) services provide the capability for all radio communication devices to transmit and receive efficiently. Radio communication devices in a given area must cooperate if they are to avoid interference problems. If they operate on the same frequencies, at the same time and in the same area, their transmissions produce interference in each other's receivers. RF services regulate the spectrum and controls access because of the potential for interference between uncoordinated uses.

Frequency management provides guidance and support for the assignment, management, and use of radio frequencies used by all elements of the VA. The most common use for VA frequency management is mobile communications, using Ultra High Frequency (UHF) and Very High Frequency (VHF). As the demand for frequency usage has increased, technology has developed radios that can perform the same function at higher unused frequencies or with decreased bandwidth at the same frequency. The VA is converting wideband 25-kilohertz (kHz) channels to narrowband 12.5 kHz channels. The conversion doubles the number of channels and provides communications capability for more users.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Approval		The use and acquisition of all VA telecommunications radio equipment shall be approved by the National Telecommunications and Information Administration (NTIA) Interdepartmental Radio Advisory Committee.
Assignment Duration		Radio frequency assignments shall be valid for five years.

Guidelines and Best Practices

No guidelines have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	Network Management Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.260) Rational Asset Manager

General Information

Website: http://www-01.ibm.com/software/awdtools/ram/

Description: Rational Asset Manager is a collaborative software asset management tool used to manage any type of software development asset including SOA and systems development assets. Rational Asset Manager supports the Reusable Asset Specification to define, create, and modify software assets.

Decision: Approved

Decision Constraints: Contact the Software Engineering Tools Management Division for details on the constraints for use of this technology.

Decision Source: ARB

Decision Process: TRM v4

Decision Date: 9/16/2009

Current Status: Analysis Completed

Introduced By: Enterprise Tools Management

Vendor Name: IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	868: Software Configuration Management

Operating Systems Supported

- AIX
- Red Hat Linux
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Rational ClearQuest with MultiSite related as: (Companion)
- Rational ClearCase with MultiSite related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
7.0	6/28/2007		
7.1.0	7/11/2008		
7.2 (est)	10/1/2009		

VA Forecast Information (07/23/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
7.1.0	None	None	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Adoption Benefits

- Centralized repository that catalogs usable software assets provides reuse, reduces redundancy.

Adoption Risks

- None significant.

Architectural Benefits

- Integrates with other Rational development tools, i.e. Rational ClearQuest and ClearCase.

Architectural Risks

- None significant.

Standards Traceability

- Supports Reusable Asset Specification (RAS).

Tool Usage

- Development
- Management/Collaboration

General Assessment

Expected Usage:	Manage software development assets.
Assessment Type:	New
Assessment Date:	7/31/2009

Notes: Rational Asset Manager requires an application server and database. Currently supported application servers are:

- WebSphere V6.1
- Apache Tomcat V5.5

Currently supported databases are:

- SQL Server 2005
- Oracle 10g, 11g
- DB2 Enterprise Ed. 8.2, 9.1, 9.5

Asset Manager can also be installed into an existing Eclipse IDE for several Rational Eclipse based technologies and also has a web client.

Recommendation: Approve-Conditional

Recommendation Constraints: The use of required, embedded Tomcat or WebSphere applications servers for this software is restricted to environments controlled by Enterprise Tools Management.

Recommendation Justification: Rational Asset Manager provides a centralized repository for software asset definition, identification, and categorization. Rational Asset Manager integrates with other Rational products to provide version control and workflow for asset management oversight.

2.261) Rational Build Forge

General Information

Website: http://www-01.ibm.com/software/awdtools/buildforge/enterprise/

Description: Build Forge (Enterprise Edition) is a build management system providing the ability to create repeatable build, test, and release processes. Build Forge has a full security model providing role based authentication, build logging, monitoring and audit trails as well as adaptors to integrate with testing and issue management applications. Build Forge is unique with its combination of access controls, workflow based builds, and build agents that can create "target platform" builds.

Decision: Approved

Decision Constraints: Contact the Software Engineering Tools Management Division for details on the constraints for use of this technology.

Decision Source:	ARB
Decision Process:	TRM v3
Decision Date:	1/7/2009
Current Status:	Analysis Completed
Introduced By:	Enterprise Tools Management
Vendor Name:	IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	868: Software Configuration Management

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Eclipse - ***(required for some configurations)***
- SQL Server - ***(required for some configurations)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Eclipse related as: (Companion)
- Rational Functional Tester related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
7.0.0	6/21/2006		
7.0.2	7/16/2008		

VA Forecast Information (11/18/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008				CY2009				CY2010			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
7.0.0	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
7.0.2	None	None	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Architectural Area

- Integration
- Application

Architectural Benefits

- The ability to create a "target platform" build is a differentiator for Build Forge. For example, a HeV team that works in Windows for development can send the build to a Red Hat server for compilation in the destination operating environment.
- Enterprise features that allow for internal-external separation of build elements. Build Forge has capabilities to securely accommodate the mix of software created by the VA and by external contractors.
- Access controls to build objects. Build Forge is distinguished from open source tools in that it can control access to objects that compose the build. In Build Forge, each object has permission attributes. That means it is possible to hide sensitive information, (such as a password setting) and restrict access to that attribute for a specific user or group.

Architectural Risks

- Vendor lock-in. Build Forge is a commercial tool.

EA Requirement

- ENTR 1074 - Implement a One VA information technology framework that supports the integration of information across business lines and that provides a source of consistent, reliable, accurate, and secure information to veterans and their families, employees, and stakeholders (Enabling Objective E-3).

Tool Type

- Platform
- Commercial

Tool Usage

- Management/Collaboration
- Development

General Assessment

Expected Usage:	Distributed software builds.
Assessment Type:	New
Assessment Date:	11/18/2008
Notes:	This assessment covers both the Enterprise and Standard configurations of Build Forge. Build Forge Standard Edition offers

	all of the functionality of Enterprise with the exception of the distributed build agents.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Build Forge is not as familiar to developers as some of the open source tools (Build Forge is not free); but when viewed from the enterprise perspective it has distinct advantages: a full security model with role based authentication, compliance audit trails, integration with OED testing and issue management applications, and the ability to create "target platform" builds.

2.262) Rational ClearCase with MultiSite

General Information

Website:	http://www-306.ibm.com/software/awdtools/clearcase/
Description:	Rational ClearCase is a software configuration management solution that provides version control, workspace management, and build auditing. ClearCase supports parallel development and, coupled with MultiSite, geographically distributed development.
Decision:	Approved
Decision Constraints:	Contact the Software Engineering Tools Management Division for details on the constraints for use of this technology.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	868: Software Configuration Management

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***
- Eclipse - ***(required for some configurations)***

Comparable Technologies/Standards:

- Rational Team Concert

Companion Technologies/Standards:

- Rational ClearQuest with MultiSite related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2003.06	10/1/2003	9/30/2008	
7.0.0.0	6/6/2006		

7.0.1.0	7/1/2007		
7.0.2 (est)	4/1/2009		
7.0.3 (est)	4/1/2010		
8.0 (est)	9/30/2010		

VA Forecast Information (09/25/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008				CY2009				CY2010			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2003.06	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
7.0.0.0	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**
7.0.2 (est)	None	None	None	None	None	None	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Architectural Area

- Application

Architectural Benefits

- The deployment and use of a standard software configuration management solution provides a common toolset which leads to improvements in efficiency.

Architectural Risks

- The ClearCase solution has a relatively high learning curve and requires significant management overhead in terms of computing resources and personnel.

Tier Used

- Infrastructure Tier

Tool Type

- Tool

Tool Usage

- Management/Collaboration
- Development

General Assessment

Expected Usage:	ClearCase is a software configuration management tool to manage code baselines providing version control, build and workspace management, and parallel development support.
Assessment Type:	Refresh
Assessment Date:	9/25/2008
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	A standardized software configuration management solution provides a consistent approach to develop and deliver HeV solutions.

2.263) Rational ClearQuest with MultiSite

General Information

Website:	http://www-01.ibm.com/software/awdtools/clearquest/
Description:	Rational ClearQuest is a workflow engine used primarily for change request, issue and risk tracking. ClearQuest integrates with

	requirements, development, build, test, and deployment tools from IBM-Rational.
Decision:	Approved
Decision Constraints:	Contact the Software Engineering Tools Management Division for details on the constraints for use of this technology.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	868: Software Configuration Management

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Eclipse - ***(required for some configurations)***
- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Rational RequisitePro related as: (Companion)
- Rational TestManager related as: (Companion)
- Rational ClearCase with MultiSite related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2003.06	1/10/2003 12:17:00 AM	9/30/2008	
7.0.0.0	6/6/2006		
7.0.1.0	9/27/2007		
7.0.2 (est)	4/1/2009		
7.0.3 (est)	4/1/2010		
8.0 (est)	9/30/2010		

VA Forecast Information (10/03/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008				CY2009				CY2010			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**

2003.06	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
7.0.1.0	None	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
7.0.2 (est)	None	None	None	None	None	None	None	None	Planning	Evaluation	Supported	Supported
Forecast Note:												

General Analysis

Architectural Area

- Application

Architectural Benefits

- The deployment and use of a standard workflow engine for change requests-issue tracking leads to improvements in efficiency.

Architectural Risks

- The ClearQuest solution has a relatively high learning curve and requires significant resources to operate-maintain.

EA Requirement

- ENTR 1074: VA OBJECTIVE E.3 Implement a One-VA information technology framework that enables the consolidation of IT solutions and the creation of cross-cutting common services to support the integration of information across business lines and provides secure, consistent, reliable, and accurate information to all interested parties.

Tier Used

- Infrastructure Tier

Tool Type

- Tool

Tool Usage

- Management/Collaboration

- Development

General Assessment

Expected Usage:	ClearQuest is a workflow tool used to manage defects, issues, and change request records for software development efforts. MultiSite is the data distribution component that enables geographically dispersed teams access to ClearQuest databases via replications to distributed servers.
Assessment Type:	Refresh
Assessment Date:	10/3/2008
Notes:	Link to Forrester evaluation of SCCM (Software Change and Configuration Management) products from Q2, 2007: ftp://ftp.software.ibm.com/software/rational/web/reports/forrester_scm_wave_2007.pdf
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	A standardized change management solution fosters a consistent approach to develop and deliver HeV solutions.

2.264) Rational Functional Tester

General Information

Website:	http://www-01.ibm.com/software/awdtools/tester/functional/
Description:	Rational Functional Tester is an automated testing framework that provides functional, regression, GUI, and data-driven testing capabilities.
Decision:	Approved
Decision Constraints:	Contact the Software Engineering Tools Management Division for details on the constraints for use of this technology.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008

Current Status: Analysis Completed
Introduced By: TRM Team
Vendor Name: IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	869: Test Management

Operating Systems Supported

- Red Hat Linux
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Rational TestManager related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2003.06	10/17/2003	9/30/2008	
6.1	1/7/2005	4/30/2008	
7.0.0	12/22/2006		
7.0.1	10/31/2007		
8 (est)	4/1/2009		

VA Forecast Information (10/03/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008				CY2009				CY2010			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2003.06	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
7.0.1	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
8 (est)	None	None	None	None	None	None	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Architectural Area

- Application
- Data
- Integration

Architectural Benefits

- The use of a standard functional testing tool fosters improvements in efficiency.

Architectural Risks

- None significant

Tier Used

- Tier Usage Areas

Tool Type

- Tool
- Framework

Tool Usage

- Development

General Assessment

Expected Usage:	Rational Functional Tester is an automated testing framework that provides the capability for functional and regression testing for software development efforts.
Assessment Type:	Refresh
Assessment Date:	10/3/2008
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Functional Tester provides a consistent framework for automated testing and is a standard in the Rational Suite.

2.265) Rational Manual Tester

General Information

Website: http://www-01.ibm.com/software/awdtools/tester/manual/

Description:	Rational Manual Tester provides the capability to manage manual software testing processes. Manual Tester provides test step reuse, automated keywords, and data driven tests. Manual Tester integrates with Rational ClearQuest for defect-issue documentation during the testing process.
Decision:	Approved
Decision Constraints:	Contact the Software Engineering Tools Management Division for details on the constraints for use of this technology.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	TRM Team
Vendor Name:	IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	869: Test Management

Operating Systems Supported

- Red Hat Linux
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required for some configurations)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Rational TestManager related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
6.1	1/7/2005	4/30/2008	
7.0.0	12/8/2006		
7.0.0.1	1/31/2008		
7.0.0.2	3/7/2007		
7.0.1.0	10/26/2007		
7.0.1.1	12/19/2007		
7.0.1.2	3/7/2008		
7.0.2 (est)	1/31/2009		
8.0 (est)	10/1/2009		

VA Forecast Information (10/09/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008				CY2009				CY2010			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
7.0.	**Deprec**	**Deprec**	**Deprec**	**Deprec**	**Deprec**	**Depre**	**Depre**	**Depre**	**Depre**	**Depre**	**Depre**	**Depre**

0.1	ated	ated	ated	ated	ated	cated	cated	cated	cated	cated	cated	cated
7.0.0.2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated
7.0.1.2	None	None	None	None	None	Planning	Planning	Evaluation	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Architectural Area

- Application
- Data
- Integration

Architectural Benefits

- A standard manual testing tool provides a common toolset, reducing the learning curve for HeV projects.

Architectural Risks

- Vendor lock-in: test data is stored in a proprietary format.

Tier Used

- Infrastructure Tier

Tool Type

- Tool

Tool Usage

- Management/Collaboration
- Development

General Assessment

Expected Usage: Rational Manual Tester is a testing tool that provides the ability to develop and manage manual test routines for software development efforts.

Assessment Type: New

Assessment Date:	10/9/2008
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Rational Manual Tester is available for use by HeV projects as a component of the Rational Tools suite.

2.266) Rational Performance Tester

General Information

Website:	http://www-01.ibm.com/software/awdtools/tester/performance/
Description:	Rational Performance Tester provides performance test automation capabilities to identify and remove bottlenecks and address scalability for web and server based software applications.
Decision:	Approved
Decision Constraints:	Contact the Software Engineering Tools Management Division for details on the constraints for use of this technology.
Decision Source:	ARB
Decision Process:	TRM v4
Decision Date:	9/16/2009
Current Status:	Analysis Completed
Introduced By:	Enterprise Tools Management
Vendor Name:	IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	869: Test Management

Operating Systems Supported

- Red Hat Linux
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Eclipse - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Rational Quality Manager related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2003.06	10/17/2003	4/30/2008	
6.1	5/20/2005	9/30/2008	
7.0	2/19/2007		
8.0	10/28/2008		
8.1	7/14/2009		

VA Forecast Information (08/10/2009)

The VA Forecast offers the current and future VA IT position regarding different

releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
7.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
8.1	Evaluation	Planning	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:	Planning and evaluation was started with version 8.0, as version 8.1 was released during the evaluation phase.											

General Analysis

Adoption Benefits

- The use of performance testing software leads to increased maturity of both deployed solutions and the development organization.

Adoption Risks

- None significant.

Architectural Benefits

- Feedback from performance testing efforts validates the scalability or exposes shortcomings of the design architecture.

Architectural Risks

- None significant.

Tool Type

- Testing/Development

General Assessment

Expected Provide performance testing capabilities.

Usage:	
Assessment Type:	New
Assessment Date:	8/13/2009
Notes:	The Rational Performance Tester (RPT) client is an Eclipse based application. Check specific release notes to determine the supported Eclipse version. The Rational Performance Tester Agent component is supported on AIX, in addition to Linux and Windows operating systems. The RPT agent component is used to simulate user sessions on remote systems. Rational Performance Tester offers several extensions for specific software environments such as SAP, Citrix, and Siebel. Note that the SAP and Citrix extensions are only supported on Microsoft Windows platforms.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Rational Performance Tester is part of the suite of Rational products currently offered and supported by the Enterprise Tools Management Division and is being used by existing HeV project teams.

2.267) Rational PurifyPlus

General Information

Website:	http://www-01.ibm.com/software/awdtools/purifyplus/
Description:	Rational PurifyPlus
Decision:	Approved
Decision Constraints:	Contact the Software Engineering Tools Management Division for details on the constraints for use of this technology.
Decision Source:	HSD&D
Decision Process:	ETL

Decision Date: 12/1/2006
Current Status: Introduced
Introduced By: Extended Tool List (ETL)
Vendor Name: IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	869: Test Management

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (08/10/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:	Planning and evaluation was started with version 8.0, as version 8.1 was released during the evaluation phase.											

General Analysis

ETL Approved Technology/Standard, TRM Analysis still pending.

General Assessment

ETL Approved Technology/Standard, TRM Assessment still pending.

2.268) Rational Quality Manager

General Information

Website: http://www-01.ibm.com/software/awdtools/rqm/

Description: Rational Quality Manager is a web-based centralized test management environment for test planning, workflow control, tracking and metrics reporting.

Decision: Approved

Decision Constraints: Contact the Software Engineering Tools Management Division for details on the constraints for use of this technology.

Decision Source: ARB

Decision Process:	TRM v4
Decision Date:	9/16/2009
Current Status:	Analysis Completed
Introduced By:	Enterprise Tools Management
Vendor Name:	IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	869: Test Management

Operating Systems Supported

- Red Hat Linux
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Internet Explorer - ***(required for some configurations)***
- Firefox - ***(required for some configurations)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Rational Team Concert related as: (Companion)
- Rational Requirements Composer related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	12/18/2008		
2.0	7/29/2009		

VA Forecast Information (08/06/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2.0	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Adoption Benefits

- The RQM platform takes advantage of the next generation data model that provides tighter integration and richer capabilities for project management/oversight.

Adoption Risks

- The RQM platform is a test management environment providing test planning, workflow control, tracking and metrics reporting. The potential for significant learning curve exists.

Architectural Benefits

- None significant.

Architectural Risks

- None significant.

Tool Type

- Platform

Tool Usage

- Software Development/Testing
- Management/Collaboration

General Assessment

Expected Usage:	Rational Quality Manager is a software testing and quality assurance platform used by QA teams to manage quality assurance efforts.
Assessment Type:	New
Assessment Date:	8/10/2009
Notes:	Rational Quality Manager Standard Edition comes with Rational Test Lab Manager. Rational Quality Manager requires an application server and database. Currently supported application servers are: • Websphere V6.1 • Websphere V7.0 • Apache Tomcat V5.5 Currently supported databases are: • SQL Server 2005 • SQL Server 2008 • Oracle 10g • Apache Derby • DB2 Enterprise Ed. 9.1, 9.5
Recommendation:	Approve-Conditional

Recommendation Constraints:	The use of required, embedded Tomcat or WebSphere applications servers for this software is restricted to environments controlled by Enterprise Tools Management.
Recommendation Justification:	Rational Quality Manager provides an integrated platform for software test creation, management, and execution. Rational Quality Manager is integrated with Rational Team Concert, Rational Requirements Composer, and other Rational testing tools to provide quality assurance oversight into the software development process.

2.269) Rational Requirements Composer

General Information

Website:	http://www-01.ibm.com/software/awdtools/rrc/
Description:	Rational Requirements Composer, which is based on IBM's Jazz architecture, is a requirements management platform that enables organizations to create or enhance requirements processes and provides visualization and collaboration capabilities.
Decision:	Approved
Decision Constraints:	Contact the Software Engineering Tools Management Division for details on the constraints for use of this technology.
Decision Source:	ARB
Decision Process:	TRM v4
Decision Date:	9/16/2009
Current Status:	Analysis Completed
Introduced By:	Enterprise Tools Management
Vendor Name:	IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	870: Modeling

Operating Systems Supported

- Red Hat Linux
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Internet Explorer - ***(required for some configurations)***
- Firefox - ***(required for some configurations)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Rational Quality Manager related as: (Companion)
- Rational Team Concert related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	9/12/2008		
2.0 (est)	12/31/2009		

VA Forecast Information (08/05/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or

production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.0	None	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
2.0 (est)	None	None	None	None	Evaluation	Planning	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Adoption Benefits

- The RRC platform takes advantage of the next generation data model that provides tighter integration and richer capabilities for project management/oversight.

Adoption Risks

- The RRC platform provides requirements management and visualization and collaboration capabilities. The potential for significant learning curve exists.

Architectural Benefits

- None significant.

Architectural Risks

- None significant.

Tool Type

- Platform

Tool Usage

- Development
- Management/Collaboration

General Assessment

Expected Usage:	Integrated and collaborative solution for requirements management.
Assessment Type:	New
Assessment Date:	8/6/2009
Notes:	While Rational Requirements Composer replaces the functionality of Rational Requisite Pro, there are integration connectors that provide bridges to those tools for side by side use. This allows projects currently using Rational Requisite Pro to migrate to Rational Requirements Composer at a measured pace. The server component of Rational Requirements Composer depends on a database server and application server. Current supported database servers are: • DB2 v9.5 • DB2 v9.1 • Oracle 10g Current supported database servers are: • Websphere Application Server v6.1 • Apache Tomcat v5.5
Recommendation:	Approve-Conditional
Recommendation Constraints:	The use of required, embedded Tomcat or WebSphere applications servers for this software is restricted to environments controlled by Enterprise Tools Management.
Recommendation Justification:	Rational Requirements Composer represents the next generation of requirements management platform with reporting and dashboard capabilities as well as tight integration to other Rational products based on Jazz, specifically Rational Team Concert and Rational Quality Manager.

2.270) Rational RequisitePro

General Information

Website:	http://www-01.ibm.com/software/awdtools/reqpro/
Description:	Rational RequisitePro is a requirements management solution used by software development teams. It provides a common repository for storing and managing requirements and use cases. RequisitePro integrates with other tools in the Rational suite.
Decision:	Approved
Decision Constraints:	Contact the Software Engineering Tools Management Division for details on the constraints for use of this technology.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	870: Modeling

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Rational ClearCase with MultiSite related as: (Companion)
- Rational ClearQuest with MultiSite related as: (Companion)
- Rational TestManager related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2003.06	10/17/2003	9/30/2008	
7.0.0.0	6/1/2006		
7.0.1.0	10/31/2007		
7.0.1.2	9/30/2008		

VA Forecast Information (11/06/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008				CY2009				CY2010			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
7.0.	**Deprec**	**Deprec**	**Deprec**	**Deprec**	**Deprec**	**Deprec**	**Deprec**	**Depre**	**Depre**	**Depre**	**Depre**	**Depre**

0.0	ated	ated	ated	ated	ated	ated	ated	cated	cated	cated	cated	cated
7.0.1.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated
7.0.1.2	None	None	None	None	None	None	None	Planning	Evaluation	Supported	Supported	Supported
Forecast Note:												

General Analysis

Architectural Area

- Application

Architectural Benefits

- Rational RequisitePro provides traceability to application and enterprise architecture requirements.

Architectural Risks

- None significant.

EA Requirement

- ENTR 1074 - Implement a One VA information technology framework that supports the integration of information across business lines and that provides a source of consistent, reliable, accurate, and secure information to veterans and their families, employees, and stakeholders (Enabling Objective E-3).

Tier Used

- Infrastructure Tier

Tool Type

- Tool

Tool Usage

- Management/Collaboration
- Development

General Assessment

Expected Usage:	Rational RequisitePro is a tool to manage requirements and use cases for software development efforts.
Assessment Type:	Refresh
Assessment Date:	11/6/2008
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	A standardized requirements management solution provides a consistent approach to document requirements. Rational RequisitePro is currently in use and being adopted across many VA projects.

2.271) Rational Robot

General Information

Website:	http://www-01.ibm.com/software/awdtools/tester/robot/index.html
Description:	Rational Robot
Decision:	Approved
Decision Constraints:	Contact the Software Engineering Tools Management Division for details on the constraints for use of this technology.
Decision Source:	HSD&D
Decision Process:	ETL
Decision Date:	12/1/2006
Current Status:	Introduced
Introduced By:	Extended Tool List (ETL)
Vendor Name:	IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
N/A	N/A	N/A

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (11/06/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be

supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

ETL Approved Technology/Standard, TRM Analysis still pending.

General Assessment

ETL Approved Technology/Standard, TRM Assessment still pending.

2.272) Rational Rose

General Information

Website: http://www-01.ibm.com/software/awdtools/developer/rose/index.html

Description: Rational Rose

Decision: Approved

Decision Constraints: Contact the Software Engineering Tools Management Division for details on the constraints for use of this technology.

Decision Source: HSD&D

Decision Process: ETL

Decision Date: 12/1/2006

Current Status: Introduced

Introduced By: Extended Tool List (ETL)

Vendor Name: IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	870: Modeling

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Rational Software Modeler
- Rational Software Architect

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (11/06/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be

supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

ETL Approved Technology/Standard, TRM Analysis still pending.

General Assessment

ETL Approved Technology/Standard, TRM Assessment still pending.

2.273) Rational RUP

General Information

Website:	http://www-01.ibm.com/software/awdtools/rup/index.html
Description:	Rational RUP
Decision:	Approved
Decision Constraints:	Contact the Software Engineering Tools Management Division for details on the constraints for use of this technology.
Decision Source:	HSD&D
Decision Process:	ETL
Decision Date:	12/1/2006
Current Status:	Introduced
Introduced By:	Extended Tool List (ETL)
Vendor Name:	IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	870: Modeling

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- Eclipse - ***(required for some configurations)***
- JRE - Sun - ***(required for some configurations)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (11/06/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be

supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

ETL Approved Technology/Standard, TRM Analysis still pending.

General Assessment

ETL Approved Technology/Standard, TRM Assessment still pending.

2.274) Rational Software Architect

General Information

Website:	http://www-01.ibm.com/software/awdtools/architect/swarchitect/
Description:	Rational Software Architect (RSA) is one of the most advanced off-the-shelf software development tools available. Based on the Eclipse platform, this product offers a plethora of UML modeling, software architecture, design, and software construction functionality.
Decision:	Approved
Decision Constraints:	Contact the Software Engineering Tools Management Division for details on the constraints for use of this technology.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Introduced
Introduced By:	Enterprise Tools Management
Vendor Name:	IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	867: Integrated Development Environments (IDE)

Operating Systems Supported

- Red Hat Linux
- Windows (Client)

Technologies/Standards Relationships

Runtime Dependencies:

- Eclipse - ***(required libraries)***
- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- Rational Software Modeler
- Rational Rose
- MyEclipse

Companion Technologies/Standards:

- Rational Systems Developer related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date

7.0.0.1	1/31/2007		
7.0.0.2	4/9/2007		
7.0.0.3	6/29/2007		
7.0.0.4	9/28/2007		
7.0.0.5	12/11/2007		
7.0.0.6	3/28/2008		
7.0.0.7	6/26/2008		
7.0.0.8	12/11/2008		
7.5	9/26/2008		
7.5.1	12/11/2008		

VA Forecast Information (10/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
7.0.0.5	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
7.5	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Architectural Area

- Application

Architectural Benefits

- Support for HTML, DHTML, XHTML, CHTML, JavaScript, CSS
- Support for building J2EE applications
- Integrated deployment of J2EE applications to a WebLogic server
- Support for JAR, EAR, WAR packaging

Architectural Risks

- Potential for vendor lock-in
- Better integration with IBM WebSphere than WebLogic

EA Requirement

- ENTR 1074 - Implement a One VA information technology framework that supports the integration of information across business lines and that provides a source of consistent, reliable, accurate, and secure information to veterans and their families, employees, and stakeholders (Enabling Objective E-3).

Standards Traceability

- EJB 1.1, 2.0, 2.1
- JAXP 1.2 (J2EE 1.4), 1.3 (J2SE 5)
- SOAP 1.1, 1.2
- JNDI 1.2.1
- JSP 1.1, 1.2, 2.0
- J2EE 1.2, 1.3, 1.4
- JDBC 3.0
- Servlet 2.3, 2.4

Tier Used

- Other Tier

Tool Type

- Commercial

Tool Usage

- Development

General Assessment

Expected Usage:	IDE
Assessment Type:	Refresh
Assessment Date:	2/6/2009
Notes:	The Rational tools: Software Modeler, Systems Developer, Application Developer contain subsets of the functionality found in

	Rational Software Architect. Rational Software Architect is commonly called "RSA", and the suite of products based on RSA is often referred to as "RsX".
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Rational Software Architect is in the current baseline of tools offered by the OED Tools Management Division.

2.275) Rational Software Modeler

General Information

Website:	http://www-01.ibm.com/software/awdtools/modeler/swmodeler/index.html
Description:	Rational Software Modeler (RSM) is a UML 2.0 based modeling and design tool. Built on top of the Eclipse platform, this product offers a plethora of UML modeling and software design-construction functionality. RSM contains a subset of Rational Software Architect.
Decision:	Approved
Decision Constraints:	Contact the Software Engineering Tools Management Division for details on the constraints for use of this technology.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Introduced
Introduced By:	Enterprise Tools Management
Vendor Name:	IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	867: Integrated Development Environments (IDE)

Operating Systems Supported

- Red Hat Linux
- Windows (Client)

Technologies/Standards Relationships

Runtime Dependencies:

- Eclipse - ***(required libraries)***
- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- Rational Rose

Companion Technologies/Standards:

- Rational Software Architect related as: (Companion)
- Rational Systems Developer related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
7.0	12/5/2006		
7.0.0.2	4/9/2007		
7.0.0.4	9/28/2007		
7.0.5.0	12/14/2007		

7.0.5.1	3/27/2008		
7.0.5.2	6/26/2008		
7.0.5.3	12/11/2008		
7.5	10/1/2008		
7.5.1	12/11/2008		
8.0 (est)	9/30/2009		

VA Forecast Information (10/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
7.0	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
7.0.5.0	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
7.5	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. The Benefits Segment use of Software Modeler is currently based on version 7.5.

General Analysis

Architectural Area

- Application

Architectural Benefits

- Support for HTML, DHTML, XHTML, CHTML, JavaScript, CSS
- Support for building J2EE applications
- Deploy J2EE applications to WebLogic server
- Support for JAR, EAR, WAR packaging

Architectural Risks

- Potential for vendor lock-in
- Better integration with IBM WebSphere than WebLogic

EA Requirement

- ENTR 1074 - Implement a One VA information technology framework that supports the integration of information across business lines and that provides a source of consistent, reliable, accurate, and secure information to veterans and their families, employees, and stakeholders (Enabling Objective E-3).

Standards Traceability

- EJB 1.1, 2.0, 2.1
- JAXP 1.2 (J2EE 1.4), 1.3 (J2SE 5)
- SOAP 1.1, 1.2
- JNDI 1.2.1
- JSP 1.1, 1.2, 2.0
- J2EE 1.2, 1.3, 1.4
- JDBC 3.0
- Servlet 2.3, 2.4

Tier Used

- Other Tier

Tool Type

- Commercial

Tool Usage

- Development

General Assessment

Expected Usage:	IDE
Assessment Type:	Refresh
Assessment Date:	2/12/2009
Notes:	Rational Software Modeler contains a subset of functionality of Rational Software Architect, as do other Rational modeling tools

	such as Systems Developer and Application Developer.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Rational Software Modeler is in the current baseline of tools offered by the OED Tools Management Division.

2.276) Rational Team Concert

General Information

Website:	http://www-01.ibm.com/software/awdtools/rtc/enterprise/
Description:	Rational Team Concert is a collaborative software development/delivery environment based on IBM's Jazz technology platform. Team Concert provides software version control, workspace management and supports parallel development. IBM's Jazz technology platform is a framework that is the foundation for a suite of development and collaboration products.
Decision:	Approved
Decision Constraints:	Contact the Software Engineering Tools Management Division for details on the constraints for use of this technology.
Decision Source:	ARB
Decision Process:	TRM v3.2
Decision Date:	8/19/2009
Current Status:	Analysis Completed
Introduced By:	Enterprise Tools Management
Vendor Name:	IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	868: Software Configuration Management

Operating Systems Supported

- Red Hat Linux
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- Rational ClearCase with MultiSite
- Rational ClearQuest with MultiSite

Companion Technologies/Standards:

- Rational Requirements Composer related as: (Companion)
- Rational Quality Manager related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0.0	7/18/2008		
1.0.1	11/14/2008		
2.0.0	6/30/2009		
2.0.1 (est)	10/30/2009		

VA Forecast Information (06/25/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2.0.0	None	None	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Adoption Benefits

- The RTC platform takes advantage of next generation data model, that provides tighter integration and richer capabilities for project management/oversight.

Adoption Risks

- The RTC platform provides integrated workspace, build and change. Management capabilities. The potential for significant learning curve exists.

Architectural Benefits

- None significant.

Architectural Risks

- None significant.

EA Requirement

- ENTR1074 - Implement a One VA information technology framework that supports the integration of information across business lines and that provides a source of consistent, reliable, accurate, and secure information to veterans and their families, employees, and stakeholders (Enabling Objective E-3).

Tool Type

- Platform

Tool Usage

- Development
- Management/Collaboration

General Assessment

Expected Usage:	Rational Team Concert is a software configuration management/change management solution to be used by development teams to manage software development projects.
Assessment Type:	New
Assessment Date:	6/25/2009
Notes:	While Rational Team Concert replaces the functionality of Rational ClearCase and ClearQuest, there are integration connectors that provide bridges to those tools for side by side use. This allows projects currently using ClearCase/ClearQuest to migrate to Rational Team Concert at a measured pace. The 2.0 release of Rational Team Concert includes an Enterprise edition. Enterprise edition has some new features notably unlimited scaling and unlimited developers (Standard is limited to 250) developers. Rational Team Concert requires an application server and database. Currently supported application servers are: • Websphere V6.1 • Websphere V7.0 • Apache Tomcat V5.5 Currently supported databases are: • SQL Server 2005 • SQL Server 2008 • Oracle 10g • Apache Derby • DB2 Enterprise Ed. 9.1, 9.5
Recommendation:	Approve-Conditional

Recommendation Constraints:	The use of required, embedded Tomcat or WebSphere applications servers for this software is restricted to environments controlled by Enterprise Tools Management.
Recommendation Justification:	Rational Team Concert is IBM's next generation configuration/change management platform providing tight data integration, project management, and collaboration capabilities.

2.277) Rational TestFactory

General Information

Website:	http://www.ibm.com/software/rational/
Description:	Rational TestFactory
Decision:	Approved
Decision Constraints:	Contact the Software Engineering Tools Management Division for details on the constraints for use of this technology.
Decision Source:	HSD&D
Decision Process:	ETL
Decision Date:	12/1/2006
Current Status:	Introduced
Introduced By:	Extended Tool List (ETL)
Vendor Name:	IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	869: Test Management

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (06/25/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

ETL Approved Technology/Standard, TRM Analysis still pending.

General Assessment

ETL Approved Technology/Standard, TRM Assessment still pending.

2.278) Rational TestManager

General Information

Website:	http://www-01.ibm.com/software/awdtools/test/manager/
Description:	Rational TestManager is a central console for software testing encompassing all aspects of test execution, analysis and reporting. TestManager supports all kinds of testing from manual to automated including: unit, functional, and performance. Rational TestManager integrates out of the box with Rational Requisite Pro and Rational ClearQuest providing the capability to associate test cases with requirements and change artifacts. These integrations provide traceability between requirements and test cases and the ability to import test data-results into defect records.
Decision:	Approved
Decision Constraints:	Contact the Software Engineering Tools Management Division for details on the constraints for use of this technology.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	869: Test Management

Operating Systems Supported

- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Rational Functional Tester related as: (Companion)
- Rational RequisitePro related as: (Companion)
- Rational Manual Tester related as: (Companion)
- Rational ClearQuest with MultiSite related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2003.06	5/20/2003	9/30/2008	
7.0.0.0	6/1/2006		
7.0.1.0	7/11/2007		

7.0.1.2	8/23/2008		
7.0.2 (est)	9/30/2009		
8.0 (est)	12/1/2009		

VA Forecast Information (10/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008				CY2009				CY2010			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
7.0.0.0	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
7.0.1.0	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**
7.0.1.2	None	None	None	None	None	None	**Planning**	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Architectural Area

- Application
- Data
- Integration

Architectural Benefits

- The use of a standard test management tool leads to improvements in efficiency and establishes consistent processes for IT personnel supporting HeV.

Architectural Risks

- Vendor lock-in: test data is stored in a proprietary format.

Tier Used

- Infrastructure Tier

Tool Type

- Tool

Tool Usage

- Management/Collaboration
- Development

General Assessment

Expected Usage:	Rational TestManager is a software test management solution for test activity management, test execution and reporting.
Assessment Type:	Refresh
Assessment Date:	10/14/2008
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	TestManager is a standard in the Rational Tool suite offered by the Software Engineering Tools Management Division.

2.279) Red Hat Linux

General Information

Website:	http://www.redhat.com/rhel
Description:	Red Hat Linux is a packaged version of the open source Linux operating system. The Red Hat company provides installation routines, pre-configured components, and support services that make the installation-maintenance of the operating system easier.
Decision:	Approved
Decision	No constraints have been specified at this time.

Constraints:	
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	RedHat

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Solaris
- HP-UX
- AIX

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2.1	5/17/2002		5/31/2009
3.0	10/23/2003		10/31/2010
4.0	2/14/2005		2/28/2012
5.0	3/4/2007		3/31/2014
5.1	11/7/2007		
5.2	5/21/2008		
5.3	1/19/2009		
5.4	9/2/2009		

VA Forecast Information (11/06/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
4.0	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
5.0	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
5.1	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
5.2	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
5.3	None	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

Forecast Note:	

General Analysis

Architectural Area

- Application
- Data
- Integration

Architectural Benefits

- Operating systems which are independent of the hardware supplier provide modularity and flexibility to the deployment and physical configuration of the architecture.

Architectural Risks

- None significant.

Standards Traceability

- Redhat standard compliance information can be found at the following link: https://www.redhat.com/apps/isv_catalog

Tier Used

- Middle Tier (Business)
- Data Tier
- Presentation Tier (Thick)
- Middle Tier (Integration)
- Presentation Tier (Web)
- Client Tier
- Middle Tier (Infrastructure)

Tool Type

- Platform

Tool Usage

- Development
- Management/Collaboration
- Runtime

General Assessment

Expected Usage:	The inclusion of Red Hat Linux in TRM v2 fulfills the objectives outlined in ENTR68 (now marked as inactive).
Assessment Type:	Refresh
Assessment Date:	10/14/2008
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Recommend approval as Red Hat Linux has been successfully implemented in the HeV infrastructure.

2.280) Reflections

General Information

Website:	http://www.attachmate.com/Products/Products.htm
Description:	Reflection Suite for X is a PC X server, an NFS client, and terminal emulation software. It connects Windows users to applications on UNIX, OpenVMS, IBM, Unisys, and Linux systems. It provides easy access to NFS resources. The product also includes an SSH client to tunnel and TCP traffic.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v4
Decision Date:	9/16/2009
Current Status:	Introduced
Introduced By:	Extended Tool List (ETL)
Vendor Name:	Attachmate

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Access Channels	853: Other Electronic Channels

Operating Systems Supported

- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
14.0.5	9/1/2008		

14.0.6	4/9/2009		

VA Forecast Information (07/29/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
14.0.5	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
14.0.6	None	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Adoption Benefits

- Mature, stable product
- Integrates with all approved VA platforms

Architectural Benefits

- Secure user workstation file transfer capability
- Secure user workstation telnet capability

Standards Traceability

- FIPS 140-2
- FTP
- FTP/S
- SFTP
- XIM (I18N and XIMP)
- IPv6
- SSL 3.0/TLS 1.0

General Assessment

Expected Usage:	Secure telnet and file transfers from user workstations to OpenVMS, UNIX, LINUX, Bull System and IBM Mainframes systems.
Assessment Type:	New
Assessment Date:	7/31/2009
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Reflections is part of the standard image managed by EIE. The following justification is from the EIE Secure Host Integration Overview document: "Reflection supports almost all the systems within Veteran Affairs. The product includes FIPS certified encryption modules, support for CAC cards, and supports a majority of the host emulation types within Veteran Affairs. The products will give the different regions flexibility on how they want to implement the solution."

2.281) Regulations and Procedures for Federal Radio Frequency Management

General Information

Website:	http://www.ntia.doc.gov/osmhome/redbook/redbook.html
Description:	Regulations and Procedures for Federal Radio Frequency Management is the official source for all technical regulations relating to the use of the electromagnetic frequency spectrum.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008

Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: NTIA

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2008	1/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2008	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.282) Remote Access Protocol

General Information

Description: Remote Access services enable users at remote locations to connect to enterprise network services and applications from almost anywhere. Remote access provides contact from telecommuter sites, mobile computing, as well as technical support. Atelecommuter site is a small office with one to a few employees. It can also be atelecommuter's home office. Telecommuters can also refer to mobile users whotravel. Mobile computing allows field representatives to access office resources onthe road. Technical support can dial in to client systems to diagnose and

correctproblems remotely. One difference between a remote host and local-basedworkstations connected directly to the network is slower data transfer speeds. Userscan access the network via a Virtual Private Network (VPN) or traditional dial-up.VPNs allow users and customer's access to the VA network while providing asecure connection. Private data is encrypted for routing through the serviceprovider's network or the Internet.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Dialup		Point-to-point protocol (PPP) shall be used as the transporting network layer protocol across dialup serial point-to-point links.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
High Speed Access	Users who want higher speeds than analog can establish remote access with cable modems, DSL, or a router that has access to a WAN port.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.283) Remote Authentication Dial In User Service (RADIUS)

General Information

Website:	http://www.rfc-editor.org/cgi-bin/rfcsearch.pl
Description:	Remote Authentication Dial In User Service (RADIUS) is a protocol for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2865	6/1/2000		
RFC 3575	7/1/2003		
RFC 5080	12/1/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the

responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2865	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.284) Resource-Based Relative Value Scale (RBRVS)

General Information

Website: https://catalog.ama-assn.org/Catalog/product/product_detail.jsp?productId=prod1400027

Description: Resource-Based Relative Value Scale (RBRVS) is a schema used to determine how much money medical providers should be paid. RBRVS assigns procedures performed by a physician or other medical provider a relative value which is adjusted by geographic region. This value is then multiplied by a fixed conversion factor, which changes annually, to determine the amount of payment.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP
Vendor Name: AMA

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Current Procedural Terminology (CPT) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date

2008	11/30/2007		
2009	11/30/2008		
2010	11/30/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.285) Rich Text Format (RTF)

General Information

Website: http://www.microsoft.com/downloads/details.aspx?familyid=DD422B8D-FF06-4207-B476-6B5396A18A2B&displaylang=en

Description: The Rich Text Format (RTF) specification provides a format for text and graphics interchange that can be used with different output devices, operating environments, and operating systems.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008
Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: Microsoft

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	Native Document Formats*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Portable Document Format (PDF)
- Office Open XML

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.8	4/1/2004		
1.9.1	3/20/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.8	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.9.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.286) RoboHelp

General Information

Website: http://www.adobe.com/products/robohelp/

Description: RoboHelp is an authoring tool used to construct, deploy, and manage the help system for software applications.

Functionality includes the ability to build and maintain tables of contents, index, glossary, graphics, special effects and context-

sensitive help.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: ARB

Decision Process: TRM v3

Decision Date: 1/7/2009

Current Status: Analysis Completed

Introduced By: ARB

Vendor Name: Adobe

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
N/A	N/A	N/A

Operating Systems Supported

- Windows (Client)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.0	9/9/2002		
4.0	5/27/2003		
5.0	1/27/2004		
6.0	1/16/2007		
7.0	11/1/2007		
8.0	4/15/2009		

VA Forecast Information (11/10/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
5.0	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
6.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
7.0	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
8.0	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Architectural Area

- Application

Tier Used

- Presentation Tier

Tool Type

- Commercial

Tool Usage

- Development

General Assessment

Expected Usage:	Provides a standard solution to author and deploy help systems, knowledge bases, and other types of help documentation for desktop environments.
Assessment Type:	Refresh
Assessment Date:	4/22/2009
Notes:	The latest version of RoboHelp supports Adobe Dreamweaver, Microsoft FrontPage 2003, Homesite and Microsoft Word 2007 as well as previous versions of Word back to 2000. RoboHelp also includes a server release for delivering on line help content and for tracking how the deployed help system is accessed. However, the server release is not in the scope of this assessment.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	RoboHelp has been in use with HeV applications without issue; RoboHelp is a best-in-class solution for help file authoring.

2.287) RxNorm

General Information

Website: http://www.nlm.nih.gov/research/umls/rxnorm/docs/rxnormfiles.html

Description: RxNorm provides standard names for clinical drugs (active ingredient + strength + dose form) and for dose forms as administered to a patient. It provides links from clinical drugs, both branded and generic, to their active ingredients, drug components (active ingredient + strength), and related brand names.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: NIH

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Unique Ingredient Identifier (UNII) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	RxNorm updates are available on a weekly and monthly basis.

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.288) Scalable Vector Graphics (SVG)

General Information

Website:	http://www.w3.org/TR/SVG11/
Description:	Scalable Vector Graphics (SVG) is a family of specifications of an XML-based file format for describing two-dimensional vector graphics, both static and dynamic (i.e. interactive or animated).
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.1	1/14/2003		
1.2 (Tiny)	12/22/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
1.2 (Tiny)	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.289) Secure Code Design

General Information

Description: Secure code design is a set of engineering principles for designing system security. These principles provide a foundation upon which a more consistent and structured approach to the design, development, and implementation of IT security capabilities can be constructed. While the primary focus of these principles is the implementation of technical controls, these principles highlight the fact that, to be effective, a system security design should also consider non-technical issues, such as policy, operational procedures, and user education.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
NIST SP 800-27	Engineering Principles for Information Technology Security (EP-ITS)

	presents a list of system-level security principles to be considered in the design, development, and operation of an information system.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Security Controls*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.290) Secure Hash Standard (SHS)

General Information

Website:	http://csrc.nist.gov/publications/PubsFIPS.html
Description:	FIPS 180: This standard specifies five hash algorithms that can be used to generate digests of messages. The digests are used to detect whether messages have been changed since the digests were generated.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision	TRMSP 4.3.2

Process:
Decision Date: 3/14/2008
Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: NIST

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2	8/1/2002		
3	10/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.291) Secure Hypertext Transfer Protocol (S-HTTP)

General Information

Website: http://www.rfc-editor.org/rfcsearch.html

Description: Secure Hypertext Transfer Protocol (S-HTTP) is a protocol for securing messages sent using the Hypertext Transfer Protocol (HTTP), which forms the basis for the World Wide Web. Secure HTTP (S-HTTP) provides independently applicable security services for transaction confidentiality, authenticity/integrity and non-repudiability of origin.

Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2660	8/1/1999		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2660	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.292) Secure Remote Access with L2TP

General Information

Website: http://tools.ietf.org/html/rfc2888

Description: Secure Remote Access with L2TP extends the security

characteristics of IPsec to remote access users, as they dial-in through the Internet.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Remote Authentication Dial In User Service (RADIUS) - Standard
- Point-to-Point Protocol (PPP) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2888	8/1/2000		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2888	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.293) Secure/Multipurpose Internet Mail Extensions (S/MIME) Certificate Handling

General Information

Website:	http://www.rfc-editor.org/cgi-bin/rfcsearch.pl
Description:	Secure/Multipurpose Internet Mail Extensions (S/MIME) Certificate Handling provides a method to send and receive secure MIME messages.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2632	6/1/1999		
RFC 3580	7/1/2004		
RFC 5750	1/1/2010		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2632	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.294) Secure/Multipurpose Internet Mail Extensions (S/MIME) Message Spec

General Information

Website: http://www.rfc-editor.org/rfcsearch.html

Description: Secure/Multipurpose Internet Mail Extensions (S/MIME) provides a consistent way to send and receive secure MIME data. Based on the popular Internet MIME standard, S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption).

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.0 (RFC 2633)	6/1/1999		
3.1 (RFC 3851)	7/1/2004		
3.2 (RFC 5751)	1/1/2010		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**

Forecast Note:	

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.295) Securing Layer Two Tunneling Protocol (L2TP) with IPsec

General Information

Website:	http://tools.ietf.org/html/rfc3193
Description:	Securing Layer Two Tunneling Protocol (L2TP) with IPsec discusses how L2TP may utilize IPsec to provide for tunnel authentication, privacy protection, integrity checking and replay protection.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3193	11/1/2001		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010	CY2011	CY2012

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 3193	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.296) Security Architecture for the Internet Protocol (IP)

General Information

Website: http://tools.ietf.org/html/rfc4301

Description: Security Architecture for the Internet Protocol (IP) describes the security mechanisms for IP version 4 (IPv4) and IP version 6 (IPv6) and the services that they provide. This document also describes key management requirements for systems implementing those security mechanisms.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 1825	8/1/1995	11/1/1998	
RFC 2401	11/1/1998	12/1/2005	
RFC 4301	12/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the

responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 4301	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.297) Security Architecture for the Internet Protocol (IPSec)

General Information

Website: http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

Description: Security Architecture for the Internet Protocol (IPSec) specifies the base architecture for IPSec compliant systems. The goal of the architecture is to provide various security services for traffic at the IP layer, in both the IPv4 and IPv6 environments.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2401	11/1/1999		
RFC 4301	12/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2401	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.298) Security Assertion Markup Language (SAML)

General Information

Website: http://www.oasis-open.org/specs/#samlv2.0

Description: The Security Assertion Markup Language (SAML) specification defines the syntax and semantics for XML-encoded assertions about authentication, attributes, and authorization, and for the protocols that convey this information.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: Benefits Arch

Decision Process: TRM v4.1

Decision Date: 10/28/2009
Current Status: Analysis Completed
Introduced By: Benefits ASA
Vendor Name: OASIS

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Requirements	860: Authentication / Single Sign-on

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- WS-Security - Standard
- Extensible Markup Language (XML) - Standard
- XML Namespaces (XML-NS) - Standard
- XML Schema - Standard
- Simple Object Access Protocol (SOAP) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	11/1/2002		
1.1	8/28/2003		
2.0	2/28/2005		

VA Forecast Information (10/09/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2.0	None	None	None	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Adoption Benefits

- SAML is mature and a widely adopted industry standard.

Architectural Benefits

- SAML defines a federated identities approach that insures identities are both portable and potable, that is, they can be transported and consumed across autonomous domains or business boundaries.
- SAML is platform independent. The security framework is abstracted away from platform architectures and particular vendor implementations. Making security more independent of application logic is an important tenet of Service-Oriented Architecture.
- SAML is loose coupling of directories. User information is not required to be maintained and synchronized between directories.

- SAML defines a single sign-on approach, allowing users to authenticate at an identity provider and then access service providers without additional authentication.

General Assessment

Expected Usage:	Specification for service authentication, authorization, and single sign-on.
Assessment Type:	New
Assessment Date:	11/4/2009
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	SAML is a mature, widely adopted industry standard for federated identity. It defines standardized mechanisms for the communication of security and identity information.

2.299) Security Requirements for Cryptographic Modules

General Information

Website:	http://csrc.nist.gov/publications/PubsFIPS.html
Description:	FIPS 140: Security Requirements for Cryptographic Modules specifies the security requirements that will be satisfied by a cryptographic module. The standard provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.
Decision:	Approved
Decision	No constraints have been specified at this time.

Constraints:

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: NIST

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2	5/1/2001		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.300) Security Token

General Information

Description: A Security Token is a physical device, such as a special smart card, that together with something that a user knows, such as a PIN, enables authorized access to a computer system or network.

Decision: Approved

Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
NIST FIPS 190	Guideline For The Use Of Advanced Authentication Technology Alternatives
NIST FIPS 196	Entity Authentication Using Public Key Cryptography
NIST SP 500-157	Smart Card Technology: New Methods for Computer Access Control
NIST IR 6887	Government Smart Card Interoperability Specification
PKCS #11	Cryptographic Token Interface Standard
PKCS #15	Cryptographic Token Information Format Standard
ISO/IEC 7816-4	Organization, security and commands for interchange

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.301) Servers

General Information

Refer to document:	VA_Enterprise_Server_Standards_1_0.pdf
Description:	This standards document lists the acceptable and recommended specifications for Server Platforms. Sections include standard specifications for subject components, decisions supporting the standard specifications, guidelines or recommendations for implementing the standard specifications, and supplemental factors to consider for when evaluating subject components. Other supplementary documents will provide guidance on procuring components that meet the standard specifications, guidance on integrating them with existing components, and explanation of how the subject components fit into the VA Architecture. This standard includes the following: Light Workload Server (Class C); Typical Workload Server (Class B); Heavy Workload Server (Class A); VistA Back-End Server (Class E). For each of these standards the following supporting details are included; Processor; Performance; Memory; Internal Storage; External Storage Interface; Server Communications Interface; Removable Media Device; Power; Cooling Fan.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EIE CTO
Decision Process:	TAR-TAS

Decision Date: 11/18/2009
Current Status: Analysis Completed
Introduced By: OPS/EIE

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	877: Servers / Computers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.302) SharePoint Server

General Information

Website: http://sharepoint.microsoft.com/Pages/Default.aspx

Description: SharePoint Server, also known as Microsoft Office SharePoint Server (MOSS), is a content management system with integrated search functionality that allows users to work in a web-based collaborative environment.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	Microsoft

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Access Channels	852: Collaboration / Communications

Operating Systems Supported

- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- SQL Server - ***(required libraries)***

Comparable Technologies/Standards:

- TeamPage
- TWiki
- MediaWiki

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2003	10/21/2003		
2003 SP1	10/18/2004		
2003 SP2	10/18/2005		
2003 SP3	9/17/2007		
2007	11/7/2006		
2007 SP1	12/8/2007		
2007 SP2	7/29/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2007 SP1	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.303) Simple Mail Transfer Protocol (SMTP)

General Information

Website:	http://tools.ietf.org/html/rfc2821
Description:	Simple Mail Transfer Protocol (SMTP) is a specification of the basic protocol for the Internet electronic mail transport.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
SMTP Service Extension for Returning Enhanced Error Codes	This document defines an extension to the SMTP service whereby an SMTP server augments its responses with the enhanced mail system status codes.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2821	4/1/2001		
RFC 5336	9/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2821	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.304) Simple Network Management Protocol (SNMP)

General Information

Website:	http://tools.ietf.org/html/rfc3412
Description:	Simple Network Management Protocol (SNMP) describes the Message Processing and Dispatching for SNMP messages within the SNMP architecture. It defines the procedures for dispatching potentially multiple versions of SNMP messages to the proper SNMP Message Processing Models, and for dispatching Protocol Data Units (PDUs) to SNMP applications.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code

Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- User Datagram Protocol (UDP) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3412	12/1/2002		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo

3412	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.305) Simple Object Access Protocol (SOAP)

General Information

Website: http://www.w3.org/TR/

Description: Simple Object Access Protocol (SOAP) is a lightweight protocol intended for exchanging structured information in a decentralized, distributed environment.
SOAP is fundamentally a stateless, one-way message exchange paradigm, but applications can create more complex interaction patterns (e.g., request/response, request/multiple responses, etc.) by combining such one-way exchanges with features provided by an underlying protocol and/or application-specific information. SOAP is silent on the semantics of any application-specific data it conveys, as it is on issues such as the routing of SOAP messages, reliable data transfer, firewall traversal, etc. However, SOAP provides the framework by which application-specific information may be conveyed in an extensible manner. Also, SOAP provides a full description of the required actions taken by a SOAP node on receiving a SOAP message.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: Benefits Arch

Decision Process: TRM v4.1

Decision Date: 10/28/2009

Current Status: Analysis Completed

Introduced By: Benefits ASA

Vendor Name: W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Transport	HTTP is the preferred SOAP transport protocol.
Fault Codes	SOAP Fault Codes are the preferred method for handling problems since throwing exceptions canonly be successfully caught if the “client” is also using Java.

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Primer	Primer is a non-normative document intended to provide an easily understandable tutorial on the features of SOAP. In particular, it describes the features through various usage scenarios, and is intended to complement the normative text contained in Part 1 and Part 2 of the SOAP specifications.
Messaging Framework	Messaging Framework defines, using XML technologies, an extensible messaging framework containing a message construct that can be exchanged over a variety of underlying protocols.
Adjunts	Adjuncts defines a set of adjuncts that may be used with SOAP Messaging Framework.
Assertions and Test Collection	This document draws on assertions found in the SOAP specifications and provides a set of tests in order to show whether the assertions are implemented in a SOAP processor.
SOAP Message Transmission Optimization Mechanism (MTOM)	This document describes an abstract feature and a concrete implementation of it for optimizing the transmission and/or wire format of SOAP messages.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Extensible Markup Language (XML) - Standard
- XML-Infoset - Standard
- XML Schema - Standard
- XML Namespaces (XML-NS) - Standard
- Security Assertion Markup Language (SAML) - Standard
- WS-I Basic Profile - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.1	5/8/2000		
1.2	4/27/2007		

VA Forecast Information (09/28/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009	CY2010	CY2011

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.2	None	None	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Architectural Benefits

- Interoperability - platform independent
- Interoperability - supports multiple transport protocols (HTTP and SMTP)
- SOAP over HTTP allows for easier communication through proxies and firewalls than other remote execution technologies
- Extensible - (WS-Security is an SOAP extension)

Tier Used

- Middle Tier (Integration)

General Assessment

Expected Usage:	A standard for exchanging XML based messages over HTTP
Assessment Type:	Standard
Assessment Date:	11/3/2009
Notes:	HTTP is the preferred SOAP transport protocol since it can be more easily secured using SSL.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	SOAP is a mature, widely adopted industry standard. It is a highly interoperable messaging specification. SOAP provides a more secure approach than REST as sensitive data should not be sent as parameters in URIs.

2.306) Single Sign On

General Information

Description: Single Sign On (SSO) is a session or user authentication process that permits a user to enter one name and password in order to access multiple applications. The SSO, whichis requested at the initiation of the session, authenticates the user to access all the applications and data to which they have rights on the system, and eliminates future authentication prompts when the user switches applications during that particular session.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
NIST FIPS 48	Guidelines On Evaluation Of Techniques For Automated Personal Identification
NIST SP 800-23	Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.307) SiteMinder Web Access Manager

General Information

Website:	http://www.ca.com/us/internet-access-control.aspx
Description:	SiteMinder Web Access Manager is a suite of software components that provide single sign-on, authentication, audit and reporting for VA intranet applications.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v4
Decision Date:	9/16/2009
Current Status:	Analysis Completed
Introduced By:	TRM Team
Vendor Name:	CA

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Requirements	860: Authentication / Single Sign-on

Operating Systems Supported

- Red Hat Linux
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Active Directory related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (08/13/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be

supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**

VA forecast information is not available for this entry.

Forecast Note:	Contact the VA Identity and Access Management team for specific versions of SiteMinder covered by the VA enterprise license agreement. (http://vaww.iam.va.gov/)

General Analysis

Adoption Benefits

- SiteMinder is an enterprise scale authentication solution supported by a VA enterprise license agreement.

Adoption Risks

- None significant.

Architectural Benefits

- The SiteMinder single sign-on solution allows distributed business applications to interoperate.

Architectural Risks

- None significant.

General Assessment

Expected Usage: SiteMinder was selected independently both for Benefits Enterprise Platform and the Benefits ASA, along with the Benefits LGY Environment as the standard tool for authentication.

Assessment Type: New

Assessment Date: 8/13/2009

Notes: The scope of this assessment covers SiteMinder Web Access Manager (WAM) and these modules:

- SiteMinder WAM B to F

- SiteMinder WAM Advanced Certificate Authentication
- SiteMinder WAM Impersonation
- SiteMinder WAM Limit Concurrent Login
- SiteMinder WAM Extended NTLM Authentication
- SiteMinder WAM Override Authentication Module
- SiteMinder WAM User Context Gateway
- SiteMinder WAM SMWALKER
- SiteMinder WAM XAUTHRADIUS

Recommendation:	Approve
Recommendation Constraints:	None identified.
Recommendation Justification:	Benefits architecture is standardized on CA SiteMinder, and the VA has an enterprise license agreement for the product suite.

2.308) Solaris

General Information

Website:	http://www.sun.com/software/solaris
Description:	The Solaris Operating System (OS) is a free and open UNIX operating system. It is available for both x86 and SPARC systems. The vendor (Sun) supports the development of Solaris via the OpenSolaris project, an open source community and a place for collaboration and conversation around Solaris technology. In June 2005, Sun initiated the project by releasing the source code for the core kernel, libraries and commands of the Solaris Operating System under the terms of the OSI-approved Common Development and Distribution License (CDDL).
Decision:	Approved
Decision Constraints:	Products that have been deployed to a production environment may continue to use this technology. All other products must utilize a One-VA TRM approved Linux operating system.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed

Introduced By: TRM Team

Vendor Name: Sun Microsystems

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	866: Dependent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Red Hat Linux
- AIX
- HP-UX
- Windows (Server)

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
9 9/05	9/1/2005	4/28/2009	10/30/2014
10 1/06	1/1/2006		
10 6/06	6/1/2006		
10 11/06	11/1/2006		
10 8/07	8/1/2007		
10 5/08	5/1/2008		
10 10/08	10/31/2008		
10 5/09	5/1/2009		

VA Forecast Information (04/09/2010)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
9 9/05	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
10 6/06	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
10 11/06	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
10 8/07	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
10 10/08	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Architectural Benefits

- Solaris support for both Sun proprietary and x86 hardware greatly enhances interoperability, operations, security, and utilization of physical layer components.

Architectural Risks

- Specialized, proprietary expertise is required to build-maintain Solaris servers.

Tier Used

- Data Tier
- Middle Tier (Infrastructure)
- Middle Tier (Business)
- Middle Tier (Integration)

Tool Type

- Platform

Tool Usage

- Development
- Runtime

General Assessment

Expected Usage:	The inclusion of Solaris into the TRM fulfills the objectives outlined in ENTR68 (now marked as inactive).
Assessment Type:	Refresh
Assessment Date:	9/23/2008
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Recommend approval as Solaris is successfully implemented in the HeV infrastructure without issue.

2.309) Spring Framework

General Information

Website: http://www.springframework.org

Description: Spring is an application framework based on Inversion of Control, and provides a lightweight Java EE container. Spring is a modular framework for Java applications that can be used in a stand-alone Java Virtual Machine (JVM) with the Java SE libraries, in servlet containers, and in Java EE servers. Spring is an open source software project released under the Apache Software License.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: ARB

Decision Process: TRM v3

Decision Date: 1/7/2009

Current Status: Analysis Completed

Introduced By: Extended Tool List (ETL)

Vendor Name: SpringSource

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Core	The Core module provide the fundamental parts of the framework, including the IoC and Dependency Injection features.
Context	The Context module is a means to access objects in a framework-style manner that is similar to a JNDI registry.
Expression Language	The Expression Language module provides a powerful expression language for querying and manipulating an object graph at runtime.
JDBC	The JDBC module provides a JDBC-abstraction layer that removes the need to do tedious JDBC coding and parsing of database-vendor specific error codes.
ORM	The ORM module provides integration layers for popular object-relational

	mapping APIs, including JPA, JDO, Hibernate, and iBatis.
OXM	The OXM module provides an abstraction layer that supports Object/XML mapping implementations for JAXB, Castor, XMLBeans, JiBX and XStream.
JMS	The Java Messaging Service (JMS) module contains features for producing and consuming messages.
Transaction	The Transaction module supports programmatic and declarative transaction management for classes that implement special interfaces and for all your POJOs (plain old Java objects).
Web	Spring's Web module provides basic web-oriented integration features such as multipart file-upload functionality and the initialization of the IoC container using servlet listeners and a web-oriented application context. It also contains the web-related parts of Spring's remoting support.
Web-Servlet	The Web-Servlet module contains Spring's model-view-controller (MVC) implementation for web applications. Spring's MVC framework provides a clean separation between domain model code and web forms, and integrates with all the other features of the Spring Framework.
Web-Portlet	The Web-Portlet module provides the MVC implementation to be used in a portlet environment and mirrors the functionality of Web-Servlet module.
AOP	Spring's AOP module provides an AOP Alliance-compliant aspect-oriented programming implementation allowing you to define, for example, method-interceptors and pointcuts to cleanly decouple code that implements functionality that should be separated.
Aspects	The Aspects module provides integration with AspectJ.
Instrumentation	The Instrumentation module provides class instrumentation support and classloader implementations to be used in certain application servers.
Test	The Test module supports the testing of Spring components with JUnit or TestNG. It provides consistent loading of Spring ApplicationContexts and caching of those contexts. It also provides mock objects that you can use to test your code in isolation.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	895: Middleware

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***
- Apache Commons - ***(required libraries)***

Comparable Technologies/Standards:

- Java EE

Companion Technologies/Standards:

- Quartz Enterprise Job Scheduler related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2.0.2	1/8/2007		
2.0.3	3/9/2007		
2.0.4	4/10/2007		
2.0.5	5/7/2007		
2.0.6	6/18/2007		
2.0.7	10/1/2007		
2.0.8	1/9/2008		
2.5	11/19/2007		
2.5.4	5/1/2008		
2.5.6	10/31/2008		

VA Forecast Information (07/28/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2.5	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
2.5.4	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
2.5.6	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Architectural Area

- Application
- Data
- Integration

Architectural Benefits

- Improves the ability to test without the need for a full J2EE Container.
- Provides frameworks for Consistent Configuration and Lightweight Infrastructure components.
- Reduces compile time coupling, but leverages inversion of control and dependency injection, increasing application and architectural agility.
- Framework provides the ability to reduce J2EE Vendor Lock-in if implemented correctly.

Architectural Risks

- Learning curve; Spring uses Inversion of Control and Dependency Injection which is a different paradigm compared to core Java.
- Introduction of a specialized framework deviates from the Java EE standard. While some programming effort may be streamlined compared to EJB, the use of Spring introduces a large number of software dependencies.
- Increased maintenance effort. The use of Spring and Spring AOP can obscure program flow and make debugging more difficult.

Standards Traceability

- EJB 2.0 & 3.0
- JMX 1.2

- JPA 1.0
- JTA 1.0
- Servlet 2.3
- JCA 1.0/1.5
- JSP 1.2

Tier Used

- Middle Tier (Infrastructure)
- Client Tier
- Data Tier
- Presentation Tier (Web)
- Middle Tier (Business)
- Middle Tier (Integration)

Tool Type

- Platform
- Framework

Tool Usage

- Runtime - Embedded
- Development
- Runtime

General Assessment

Expected Usage:	The Spring Framework is designed to provide a companion and alternative to J2EE containers. Spring provides a framework and a container that works with and complements J2EE.
Assessment Type:	Re-Assess
Assessment Date:	11/6/2008
Notes:	Spring has a large number of dependencies, but the dependencies are based on how and where the Spring Framework is used; therefore, it is critical that the readme.txt file found in the Spring installation library directory is read and compared with the usage needs of the application to determine required dependencies. This will prevent dependency on a tool that may be prohibited.
Recommendation:	Approve

Recommendation Constraints:	
Recommendation Justification:	The Spring Framework is powerful and is widely used in the industry. It is included as an option in many commercial and open source J2EE application servers. The use of the Spring Framework should be controlled and the readme.txt file found in the distribution library folder should always be consulted to insure that dependencies on other libraries are approved and appropriate.

2.310) Spry Framework

General Information

Website:	http://labs.adobe.com/technologies/spry/home.html
Description:	Spry framework is an Ajax framework used for web design and development, yet is geared toward web designers. The Spry Framework has three components: Data, Widgets, and Effects. These components can be used together or independently. Spry Data provides the ability to incorporate multiple data sources into web pages. Spry Widgets are a set of web components used for styling and customization. Spry Effects provides the ability incorporate animated transitions and timed variations.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v3.2
Decision Date:	8/19/2009
Current Status:	Analysis Completed
Introduced By:	ARB
Vendor Name:	Adobe

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Data	Spry Data provides the ability to incorporate multiple data sources into web pages
Widgets	Spry Widgets are a set of web components used for styling and customization
Effects	Spry Effects provides the ability incorporate animated transitions and timed variations

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	888: Content Rendering

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- JavaScript - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- AJAX related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date

1.4	1/15/2007		
1.5	5/17/2007		
1.6	10/1/2007		
1.6.1	2/25/2008		

VA Forecast Information (07/16/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.4	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Adoption Benefits

- None significant.

Adoption Risks

- The Spry framework releases are all referred to as pre-releases, with the latest release 1.6.1, as there is no roadmap published for the Spry Framework.

Architectural Benefits

- None significant.

Architectural Risks

- None significant.

Tier Used

- Presentation Tier.

General Assessment

Expected Usage:	Pharmacy Reengineering (PRE) uses Spry widgets, specifically the tabbed panels, within edit pages.
Assessment Type:	New
Assessment Date:	7/9/2009
Notes:	The potential for accessibility issues with Spry widgets must be addressed by developers early in the life cycle.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	The Spry Framework works with any server side technology and is tool agnostic, consistent with the HeV architecture.

2.311) SQL Server

General Information

Website:	http://www.microsoft.com/sqlserver/2005/en/us/overview.aspx
Description:	SQL Server is Microsoft's relational database management system designed for the enterprise environment. Microsoft offers several editions of SQL Server including Enterprise, Workgroup, Standard, and Express.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v3
Decision Date:	1/7/2009
Current Status:	Analysis Completed
Introduced By:	ARB

Vendor Name: Microsoft

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Database/Storage	875: Database

Operating Systems Supported

- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Extensible Markup Language (XML) - ***(required for some configurations)***
- Structured Query Language (SQL) - ***(required for some configurations)***
- XQuery - ***(required for some configurations)***
- XSL Transformations (XSLT) - ***(required for some configurations)***
- XML Path Language (XPath) - ***(required for some configurations)***

Comparable Technologies/Standards:

- Oracle Database
- Cache Database Engine

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
8.0.3	1/3/2005	1/7/2003	7/10/2007
8.0.4	5/6/2005	4/8/2008	4/9/2013
9.0.0	11/7/2005	7/10/2007	7/10/2007
9.0.1	3/18/2006	4/8/2008	
9.0.2	3/5/2007	1/12/2010	
9.0.3	12/1/2007		
10.0.0	8/6/2008		

VA Forecast Information (10/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
8.0.4	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
9.0.2	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
9.0.3	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
10.0.0	Planning	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	This forecast uses the version numbers as reported by the application (refer to http://support.microsoft.com/kb/321185). Microsoft also uses this nomenclature: SQL Server 2000 (8.x); SQL Server 2005 (9.x); and SQL Server 2008 (10.x). The information displayed in the above forecast table does not apply to the Benefits Segment. The Benefits Segment use of SQL Server is currently based on version 2008 (10.0).

General Analysis

Architectural Area

- Data

Architectural Benefits

- Microsoft's SQL Server is tightly integrated with the Microsoft server, SharePoint, and the MS-Office product architecture, making integration and configuration easier than comparable database products.

Architectural Risks

- SQL Server uses T-SQL (Transact -SQL), a set of programming extensions that deviates from the ANSI SQL standard.

EA Requirement

- ENTR 1074 - Implement a One VA information technology framework that supports the integration of information across business lines and that provides a source of consistent, reliable, accurate, and secure information to veterans and their families, employees, and stakeholders (Enabling Objective E-3).
- ENTR 239 - VA Enabling Goal - Deliver World-Class Service: Deliver world-class service to veterans and their families by applying sound business principles that result in effective management of people, communications, technology, and governance

Tier Used

- Data Tier

Tool Type

- Tool
- Framework
- Commercial
- Platform

Tool Usage

- Development
- Management/Collaboration
- Runtime

General Assessment

Expected Usage:	Provide an enterprise class commercial Relational Database Management System that runs on Windows operating systems and provide the ability to store and retrieve data efficiently and securely.
Assessment Type:	New
Assessment Date:	11/18/2008
Notes:	SQL Server 2008 was recently released (8/2008) Some of the new features of the newest release include: • Backup Compression – Backup compression provides the ability to store data more effectively and reduce the storage requirements. • MERGE SQL Statement – added support for the MERGE SQL statement which is especially useful in data warehousing where data is inserted if it does not exist or updated if it does exist. MERGE is a single statement that handles both conditions. • Change Data Capture – a generic component that tracks database changes asynchronously and exposes the changes through a relational interface. This is another big enhancement in the data warehousing area where data changes need to be captured and used to update dimensions. • Table Value Parameters – provides an easier way to define a table type as well as allow applications to create, populate, and pass table structured parameters to stored procedures and functions. • Declarative Management Framework – a policy-based mechanism to ensure compliance with policies for system configuration and to prevent or monitor changes.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Microsoft SQL Server is used extensively by OED Enterprise Tools Management and by the Portal Management group. SQL Server is a cost-effective solution considering ease of use and deployment, compatibility.

2.312) Stateless Dynamic Host Configuration Protocol (DHCPv6)

General Information

Website:	http://tools.ietf.org/html/rfc3736
Description:	Stateless Dynamic Host Configuration Protocol service for IPv6 (DHCPv6) is used by nodes to obtain configuration information, such as the addresses of DNS recursive name servers, that does not require the maintenance of any dynamic state for individual clients. A node that uses stateless DHCP must have obtained its IPv6 addresses through some other mechanism, typically stateless address autoconfiguration.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3736	4/1/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 3736	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.313) Static Display

General Information

Description:	Static Display consists of the software protocols that are used to create a predefined, unchanging graphical interface between the user and the software.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Styles	When possible, use an externally linked, single style sheet (CSS) for an entire site to help enforce a consistent look and feel.
Organization	The preferred method of organizing files numbering over a few dozen is to have the directory structure mirror the major navigation of a site with graphics in a separate (images) subdirectory.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	886: Static Display

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.314) Storage

General Information

Refer to document:	VA_Enterprise_Storage_Standard_1_0.pdf
Description:	This standards document lists the acceptable and recommended specifications for general and mission critical backend storage devices, storage area network, and backup solution. Sections include standard specifications for subject components, decisions supporting the standard specifications, guidelines or recommendations for implementing the standard specifications, and supplemental factors to consider when evaluating subject components. Other supplementary documents will provide guidance on procuring components that meet the standard specifications, guidance on integrating them with existing components, and explanation of how the subject components fit into the VA Architecture. This standard includes the following: Tier 1 Storage Service; Tier 2 Storage Service; Tier 3 Storage Service; General Storage Area Network; General Backup and Archive. For each of these standards, the following supporting details are included per tier, as appropriate; Storage Subsystem Hardware; Storage Management Software; Hardware/Software Technical

	Support; Hardware/Software Installation; Training; LAN Connectivity; Fabric Switch Hardware; SAN Management Software; Backup Method; Virtual Tape Library Hardware; Archive Hardware; Tape Library Hardware; Backup Software/VTL/Archive/Tape Library Tool.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EIE CTO
Decision Process:	TAR-TAS
Decision Date:	11/18/2009
Current Status:	Analysis Completed
Introduced By:	OPS/EIE

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Database/Storage	876: Storage Devices

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.315) Strobe

General Information

Website: http://www.compuware.com/solutions/strobe.asp

Description:	Strobe measures mainframe application performance of both online and batch-processing applications while identifying chronic, recurring application failures that consume Central Processor Unit (CPU) utilization.
Decision:	Approved
Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	Compuware

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	Network Management Services*

Operating Systems Supported

- z/OS

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- BMC Mainview

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.0	4/8/2003		
3.2	3/23/2005		
4.1	2/2/2010		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
3.0	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.316) Structured Query Language (SQL)

General Information

Website: http://webstore.ansi.org/RecordDetail.aspx?sku=INCITS%2fISO%2fIEC+9075-1-2003

Description: Structured Query Language (SQL) is a database computer language designed for managing and querying data in a relational database management systems (RDBMS).

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: Benefits Arch

Decision Process: TRM v4.1

Decision Date: 10/28/2009

Current Status: Analysis Completed

Introduced By: Benefits ASA

Vendor Name: ANSI

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Framework (SQL/Framework)	ISO/IEC 9075-1 specifies the conceptual framework used in other parts of ISO/IEC 9075 to specify the grammar of SQL and the result of processing statements in that language by an SQL-implementation.
Foundation (SQL/Foundation)	ISO/IEC 9075-2 defines the data structures and basic operations on SQL-data. It provides functional capabilities for creating, accessing, maintaining, controlling, and protecting SQL-data. Both static and dynamic variants of the language are proved. In addition to direct invocation, bindings are provided for the programming languages Ada, C,

	COBOL, Fortran, M, Pascal, and PL/I.
Call-level Interface (SQL/CLI)	ISO/IEC 9075-3 defines the structures and functions that can be used to execute statements of the database language SQL from within an application written in a standard programming language in such a way that the functions used are independent of the SQL statements to be executed.
Persistent Stored Modules (SQL/PSM)	ISO/IEC 9075-4 specifies the syntax and semantics of statements to add a procedural capability to the SQL language in functions and procedures. It includes statements to direct the flow of control, define variables, make assignments and handle exception conditions.
Management of External Data (SQL/MED)	ISO/IEC 9075-9 defines extensions to SQL to support management of external data through the use of foreign-data wrappers and datalink types.
Object Language Bindings (SQL/OLB)	ISO/IEC 9075-10 defines extensions to the SQL language to support embedding of SQL statements into programs written in the Java programming language (Java is a registered trademark of Sun Microsystems, Inc.). In addition it specifies mechanisms to ensure binary portability of resulting applications.
Information and Definition Schemas (SQL/Schemata)	ISO/IEC 9075-11 specifies an Information Schema and a Definition Schema that describe: • the structure and integrity constraints of SQL-data • the security and authorization specifications relating to SQL-datathe security and authorization specifications relating to SQL-data • the features, subfeatures, and packages of ISO/IEC 9075, and the support that each of these has in an SQL implementation • the SQL-implementation information and sizing items of ISO/IEC 9075 and the values supported by an SQL-implementation
SQL Routines and Types Using Java (SQL/JRT)	ISO/IEC 9075-13 specifies the ability to invoke static methods written in the Java programming language as SQL-invoked routines and to use classes defined in the Java programming language as SQL structured user-defined types
XML-Related Specifications (SQL/XML)	ISO/IEC 9075-14 defines ways in which Database Language SQL can be used in conjunction with XML.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	895: Middleware

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- XQuery

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
SQL-86			
SQL-89			
SQL-92	7/1/1992		
SQL:1999			
SQL:2003			
SQL:2008	7/17/2008		

VA Forecast Information (10/13/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009	CY2010	CY2011

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
SQL:2003	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
SQL:2008	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Adoption Benefits

- Structured Query Language (SQL) is a mature and widely adopted industry standard for managing and querying data in a Relational Database Management Systems (RDBMS).

Adoption Risks

- The Structured Query Language (SQL) does not cover procedural languages, which are the backbone of stored procedures and triggers.
- Though vendors implement the ANSI SQL standards, the version of the standard supported may vary by vendor. Vendors also include product specific language extensions. This may result in vendor lock-in and reduce portability.

Architectural Benefits

- Standardizes the language used to manage and access Relational Database Management Systems (RDBMS).

General Assessment

Expected Usage:	Will be used as the standard language for managing and querying Relational Database Management Systems (RDBMS).
Assessment Type:	New
Assessment Date:	11/3/2009
Notes:	
Recommendation:	Approve-Conditional
Recommendation Constraints:	Hibernate Query Language (HQL) should be used for RDBMS access with java based components XQuery should be used for XML data access

Recommendation Justification:	SQL is a very mature and widely used industry standard for RDBMS data management.

2.317) Synchronous Optical Network (SONET)

General Information

Website:	http://webstore.ansi.org/RecordDetail.aspx?sku=ATIS-0900105.2008
Description:	ATIS-0900105 (formerly ANSI T1.105): Synchronous Optical Networking (SONET) or Synchronous Digital Hierarchy (SDH) are standardized multiplexing protocols that transfer multiple digital bit streams over optical fiber using lasers or light-emitting diodes (LEDs).
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ANSI

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Digital Hierarchy - Electrical	This document defines the contents of the Automatic Protection Switching (APS) bytes within the SONET signal. Formerly known as T1.105.01-

Interfaces	2000(R2005).
Jitter Network Interfaces	This document describes the jitter specifications that are applicable to SONET network and equipment interfaces (OC-N and STS-N), and jitter and wander specifications that are applicable to certain SONET payload signals (e.g. DS1 and DS3). Formerly known as T1.105.03-2003(R2008).
Automatic Protection Switching	This document defines the protocols and architectures for data communications using the DCC bytes within the SONET signal. These DCC bytes carry the OAM&P information between network elements and can be used as an integral part of the overall Telecommunications Management Network (TMN). Formerly known as T1.105.04-1995(R2005).
Tandem Connection Maintenance	This document defines the contents and use of the Tandem Connection Monitoring bytes within the SONET signal. Tandem Connection Monitoring provides enhanced maintenance capabilities for certain SONET applications. Formerly known as T1.105.02-2002(R2008).
Physical Layer Specifications	This document provides the necessary parameters for SONET optical links in short reach, intermediate reach, and long reach applications. It also provides references for the necessary parameters in SONET electrical links. Formerly known as T1.105.03-2002(R2007).
Sub STS-1 Interface Rates and Formats Specification	This document defines the formats for the VT1.5 interface and virtual tributary group interface, including the definitions and content of the associated overhead channels. Formerly known as T1.105.07-1996(R2008).
Data Communication Channel Protocol and Architectures	This document defines the SONET overhead byte locations that are used for the error correcting code and the specifications of the code itself. Formerly known as T1.105.08-2001(R2005).
Network Timing and Synchronization	This document provides timing and synchronization specifications for SONET interfaces. Compliance with this standard is necessary to achieve satisfactory interworking of telecommunications networks. Formerly known as T1.105.09-1996(R2008).

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	Metropolitan Area Network (MAN)*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1996	1/1/1996		
2005	1/1/2005		

VA Forecast Information (10/13/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.318) System for Establishing Communication Between Audiovisual Terminals

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=H

Description: ITU-T H.242: System for Establishing Communication Between Audiovisual Terminals using Digital Channels up to 2 Mbit/s describes all the point-to-point procedures involving the Bit-rate Allocation Signal (BAS) codes: initial capability exchange and mode initialization, including restricted-network operation; in-session mode switching, including audiovisual mode changes and activation of data channels; other procedures, including single/multiple channel interconnection, encryption, mode-preference indication, conveyance of network addresses and use of BAS extension codes.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code

Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
6	3/15/2004		
6.1	9/13/2005		
7	3/16/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010	CY2011	CY2012

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
6.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.319) Systematized Nomenclature of Medicine-Clinical Terms (SNOMED CT)

General Information

Website: http://www.nlm.nih.gov/research/umls/licensedcontent/snomedctfiles.html

Description: Systematized Nomenclature of Medicine-Clinical Terms (SNOMED CT) is considered to be the most comprehensive, multilingual clinical healthcare terminology in the world.

SNOMED CT was originally created by the College of American Pathologists by combining SNOMED RT and a computer based nomenclature and classification known as Clinical Terms Version 3, formerly known as Read Codes Version 3, which was created on behalf of the UK Department of Health and is Crown copyright.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IHTSDO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Technical Reference Guide	The TRG is intended for SNOMED CT implementers, such as software developers. The TRG assumes an information technology background. Clinical knowledge is not a prerequisite.
Technical Implementation Guide	The TIG is intended for SNOMED CT implementers, such as software designers. The TIG assumes information technology and software development experience. Clinical knowledge is not required, although some background is helpful to understand the application context and needs.
SNOMED CT User Guide	The User Guide is intended for clinical personnel, business directors, software product managers, and project leaders; information technology experience, though not necessary, can be helpful.
Veterans Health Administration and Kaiser Permanente (VA/KP) Problem List Subset of SNOMED CT	The Veterans Health Administration and Kaiser Permanente (VA/KP) Problem List Subset of SNOMED CT (PLS) is one of the controlled terminologies used for Structured Product Label (SPL). SPL is a document markup standard approved by Health Level Seven (HL7) and adopted by FDA as a mechanism for exchanging medication information.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Logical Observation Identifiers Names and Codes (LOINC)

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
January 2008 IR	1/31/2008		
July 2008 IR	7/31/2009		
January 2009 IR	1/31/2009		
July 2009 IR	7/31/2009		
January 2010 IR	1/31/2010		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.320) TeamPage

General Information

Website: http://www.tractionsoftware.com

Description: TeamPage is a collaborative web content development platform. It provides a hypertext platform that fosters communications among groups of contributors and consumers. TeamPage is one of the first Wiki software platforms with the initial 1.0 release shipping in 1999.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: ARB

Decision Process: TRM v3.2

Decision Date: 8/19/2009

Current Status: Introduced

Introduced By: TRM Team

Vendor Name: Traction Software

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Access Channels	852: Collaboration / Communications

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	12/1/1999		
3.5	2/1/2005		
3.7.2	12/1/2006		
4.0	11/15/2008		
4.1	2/1/2009		
4.2	2/1/2010		
4.3	2/1/2011		

VA Forecast Information (07/14/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the

responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
4.1	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
4.2	None	None	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**
4.3	None	None	None	None	None	None	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Adoption Benefits

- TeamPage would provide the VA with a commercially available Wiki platform that includes support and has been in production for nine years.
- Adoption of TeamPage would provide a platform for collaborative development of online content without the need for any specialized web development tools.

Adoption Risks

- TeamPage, as with most Wiki environments, will promote the collaborative development and publishing of online content, however this can result in content that is not officially approved by the VA and as such may require resources to monitor and moderate content.
- Adoption of a Wiki software product may add administrative overhead needed to organize, restructure and maintain content to insure its value is relevant.

Architectural Benefits

- TeamPage is written in Java which aligns with TRM standards.
- TeamPage has a stable architecture and is one of the earliest Wiki software platforms, released in 1999.

Architectural Risks

- TeamPage leverages a proprietary database, which is designed for fast storage and retrieval. It does not require any additional licensing and is fully supported by the vendor, however it is considered proprietary.

General Assessment

Expected Usage:	Provide a platform for collaborative development of web content and to promote online communications within and between groups that benefits the VA.
Assessment Type:	New
Assessment Date:	7/14/2009
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	The VA has a demonstrated need for a Wiki software platform that supports online collaborative content development that promotes communications within and among various cross functional groups. There are many Wiki software products to choose from, but few that align with the VA's currently supported Technical Reference Model. TeamPage is a hypertext platform providing Wiki functionality and targeted at collaborative online content development and communications. It is a commercial product, which will allow the VA to secure technical support should the need arise. TeamPage is written in Java and aligns with the VA's currently approved development languages. TeamPage is recommended for use where Wiki capabilities or collaborative online web content authoring is required. TeamPage is a commercial product with a long history and vendor support and it aligns with the VA Technical Reference Model.

2.321) TELNET

General Information

Website: http://tools.ietf.org/html/rfc856

Description: The TELNET Protocol provides a fairly general, bi-directional, eight-bit byte oriented communications facility. Its primary goal is to allow a standard method of interfacing terminal devices and terminal-oriented processes to each other. It is envisioned that the protocol may also be used for terminal-terminal communication ("linking") and process-process communication (distributed computation).

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	871: Web Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 854	5/1/1983		
RFC 855	5/1/1983		
RFC 856	5/1/1983		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 856	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.322) Temporal Key Integrity Protocol (TKIP)

General Information

Website: https://sbwsweb.ieee.org/ecustomercme_enu/start.swe?SWECmd=GotoView&SWEView=Catalog+View+%28eSales%29_Standards_IEEE&mem_type=Customer&SWEHo=sbwsweb.ieee.org&SWETS=1192713657

Description: Temporal Key Integrity Protocol (TKIP) is a security protocol used in the IEEE 802.11 wireless networking standard.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IEEE

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
802.11-1999			
802.11-2007			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
802.1	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo

1-1999	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.323) Teredo

General Information

Website: http://msdn.microsoft.com/en-us/library/aa965909%28v=VS.85%29.aspx

Description: Teredo is an IPv6 transition technology that provides address assignment and host-to-host automatic tunneling for unicast IPv6 traffic when IPv6/IPv4 hosts are located behind one or multiple IPv4 network address translators (NATs). To traverse IPv4 NATs, IPv6 packets are sent as IPv4-based User Datagram Protocol (UDP) messages. This article provides an overview of Teredo - including Teredo addresses and packet structures - and detailed explanations of how communication is initiated between Teredo clients, Teredo host-specific relays, and IPv6-only hosts using the IPv4 Internet, the IPv6 Internet, Teredo servers, and Teredo relays.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: Microsoft

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**

VA forecast information is not available for this entry.

Forecast Note:	See Windows Client and Windows Server for forecast information.

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.324) TOAD

General Information

Website:	http://www.quest.com/toad-for-oracle
Description:	Tool for Application Developers (TOAD) is an interactive toolset for developers to work with relational databases. It provides the functionality to build, tune, and execute queries, create and modify database objects, and develop-debug SQL and PL/SQL code.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed

Introduced By: Extended Tool List (ETL)
Vendor Name: Quest Software

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	867: Integrated Development Environments (IDE)

Operating Systems Supported

- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Oracle Database - ***(required for some configurations)***
- Windows (Client) - ***(required libraries)***
- Oracle Client - ***(required for some configurations)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
8.6.1	4/4/2006		
9.0.1	11/1/2006		
9.1	8/3/2007		
9.5	10/25/2007		
9.6	3/8/2008		
9.7	8/25/2008		

VA Forecast Information (10/09/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008				CY2009				CY2010			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
9.0.1	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
9.1	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
9.6	None	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
9.7	None	None	None	None	None	None	None	Planning	Evaluation	Supported	Supported	Supported
Forecast Note:												

General Analysis

Architectural Area

- Data
- Application

Architectural Benefits

- Common developer toolsets which support standardized skill sets, the implementation of best practices, as well as improvements in developer efficiency and effectiveness; all contribute to the architectural goals of reduced development risks and repeatable, consistent development practices for HeV.

Architectural Risks

- None significant

Tier Used

- Data Tier
- Client Tier
- Middle Tier (Infrastructure)

Tool Type

- Tool

Tool Usage

- Development
- Runtime

General Assessment

Expected Usage:	TOAD can enhance productivity with functionality focused specifically on the Oracle database.
Assessment Type:	Refresh
Assessment Date:	9/24/2008
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Recommend approval as TOAD is successfully implemented in the HeV infrastructure.

2.325) Transmission of IP Datagrams over SMDS

General Information

Website:	http://tools.ietf.org/html/rfc1209
Description:	The Transmission of Internet Protocol (IP) Datagrams over the Switched Multi-megabit Data Service (SMDS) Service describes an initial use of IP and Address Resolution Protocol (ARP) in an SMDS service environment configured as a logical IP subnetwork.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	Metropolitan Area Network (MAN)*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 1209	3/1/1991		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 1209	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.326) Transport Layer Security (TLS) Protocol

General Information

Website:	http://www.rfc-editor.org/rfcsearch.html
Description:	The Transport Layer Security (TLS) protocol provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0 (RFC 2246)	1/1/1999		
1.1 (RFC 4346)	4/1/2006		
1.2 (RFC 5246)	8/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.0 (RFC 2246)	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.327) TreeSize

General Information

Website:	http://www.jam-software.com/treesize/
Description:	TreeSize is a harddisk space manager. It shows you the size, allocated and wasted space, the number of files, 3D charts, the last access date, the file owner and permissions, the NTFS compression rate and much more information of several folders or drives you choose. It also lets you search drives, entire servers or the entire network for old, big, temporary and duplicate files.
Decision:	Approved
Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	JAM Software

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
4.3			
5.0	11/23/2007		
5.1	3/4/2008		
5.2	2/4/2009		
5.3	10/12/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the

responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
5.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.328) Triple Data Encryption Algorithm (TDEA) Block Cipher

General Information

Website: http://csrc.nist.gov/publications/PubsSPs.html

Description: Triple Data Encryption Algorithm (TDEA) Block Cipher specifies the Triple Data Encryption Algorithm (TDEA), including its primary component cryptographic engine, the Data Encryption Algorithm (DEA). When implemented in an SP 800-38 series-compliant mode of operation and in a FIPS 140-2 compliant cryptographic module, TDEA may be used by Federal organizations to protect sensitive unclassified data. Protection of data during transmission or while in storage may be necessary to maintain the confidentiality and integrity of the information represented by the data. This recommendation precisely defines the mathematical steps required to cryptographically protect data using TDEA and to subsequently process such protected data.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	NIST

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM

technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	5/1/2004		
1.1	5/19/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.329) Unified Medical Language System (UMLS)

General Information

Website: http://www.ncbi.nlm.nih.gov/bookshelf/br.fcgi?book=nlmumls

Description: The Unified Medical Language System (UMLS®) Reference Manual describes the UMLS Knowledge Sources and related tools that are produced and distributed by the National Library of Medicine, a part of the National Institutes of Health in the U.S. Department of Health and Human Services.

Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	NIH

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
MetamorphoSys	MetamorphoSys is used to create a custom Metathesaurus subset and is needed to install the most current UMLS Knowledge Sources.
UMLS Knowledge Source Server (UMLSKS)	The UMLS Knowledge Source Server (UMLSKS) provides Internet access to the three UMLS Knowledge Sources and to the UMLS tools.
Database Tools	Sample Load Scripts and Data Model
RRF Subset Browser	The RRF Subset browser provides users with an easy way to search local subsets, print concept reports, and view raw file information for a specific concept.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Red Hat Linux

- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2006 AB	11/1/2006		
2007 AA	4/1/2007		
2007 AB	11/1/2007		
2008 AA	4/1/2008		
2008 AB	11/1/2008		
2009 AA	4/1/2009		
2009 AB	11/1/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2006 AB	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	The UMLS is updated biannually in April (AA release) and November (AB release).

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.330) Uniform Resource Identifiers (URI)

General Information

Website:	http://tools.ietf.org/html/rfc3986
Description:	A Uniform Resource Identifier (URI) is a compact string of characters for identifying an abstract or physical resource. This standard defines the generic syntax of URI, including both absolute and relative forms, and guidelines for their use.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3986	1/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on

the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 3986	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.331) Unique Ingredient Identifier (UNII)

General Information

Website: http://www.fda.gov/ForIndustry/DataStandards/SubstanceRegistrationSystem-UniqueIngredientIdentifierUNII/default.htm

Description: The Unique Ingredient Identifiers (UNII) is a non-proprietary, free, unique, unambiguous, non semantic, alphanumeric identifier based on a substance's molecular structure and/or descriptive information. UNIIs are associated with substances in drugs, biologics, foods, and devices.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: FDA

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date

Vendor release information is not available for this entry.

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.332) United States Adopted Names (USAN)

General Information

Website:	http://www.ama-assn.org/ama/pub/about-ama/our-people/coalitions-consortiums/united-states-adopted-names-council/adopted-names.shtml
Description:	United States Adopted Names (USAN) are unique nonproprietary names assigned to pharmaceuticals marketed in the United States.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed

Introduced By: TRMSP

Vendor Name: AMA

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date

Vendor release information is not available for this entry.

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	Refer to the USP-NF entry for release and forecast information.

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.333) United States Pharmacopeia–National Formulary (USP–NF)

General Information

Website:	http://www.usp.org/USPNF/
Description:	The United States Pharmacopeia–National Formulary (USP–NF) is a book of public pharmacopeial standards. It contains standards for medicines, dosage forms, drug substances, excipients, medical devices, and dietary supplements.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2

Decision Date: 3/14/2008
Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: U.S. Pharmacopeia

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- United States Adopted Names (USAN) - Standard
- International Nonproprietary Names (INN) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
USP31-NF26	11/1/2007		
USP32-NF27	11/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	The USP-NF is released on November 1 of each year and becomes official on May 1 of the following year. USF33-NF28 was published on 11/2009 and recalled on 1/26/2010. The scheduled publication date is April 2010.

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.334) Universal Description, Discovery, and Integration (UDDI)

General Information

Website: http://www.oasis-open.org/committees/uddi-spec/doc/tcspecs.htm

Description: The Universal Description, Discovery, and Integration (UDDI) specification describes the Web services, data structures and behaviors of all instances of a service registry.

Decision: Approved

Decision Constraints:	No constraints have been specified at this time.
Decision Source:	Benefits Arch
Decision Process:	TRM v4.1
Decision Date:	10/28/2009
Current Status:	Analysis Completed
Introduced By:	Benefits ASA
Vendor Name:	OASIS

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
UDDI Technical Specification	This document describes the Web services and behaviors of all instances of a UDDI registry.
UDDI XML Schema	UDDI uses the XML Schema Language to formally describe its data structures: • UDDI API Schema • UDDI Custody Schema • UDDI Subscription Schema • UDDI Subscription Listener Schema • UDDI Replication Schema • UDDI Value Set Validation Schema • UDDI Value Set Caching • UDDI Policy • UDDI Policy Instance parameters
UDDI WSDL Service Interface	The complete set of UDDI WSDL definitions is provided by: • UDDI API Binding • UDDI API Port Type • UDDI Custody Binding • UDDI Custody Port Type • UDDI Replication Binding

	• UDDI Replication Port Type • UDDI Subscription Binding • UDDI Subscription Port Type • UDDI Subscription Listener Binding • UDDI Subscription Listener Port Type • UDDI Value Set Validation Binding • UDDI Value Set Caching Binding • UDDI Value Set Caching Port Type

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interface	900: Service Discovery

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Web Services Description Language (WSDL) - Standard
- Extensible Markup Language (XML) - Standard
- XML Schema - Standard
- Simple Object Access Protocol (SOAP) - Standard
- WS-I Basic Profile - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date

2.0	7/19/2002		
3.0	10/19/2004		

VA Forecast Information (10/05/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
3.0	None	None	None	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. The Benefits Segment use of the UDDI specification is currently based on version 2.0.

General Analysis

Adoption Risks

- The implementation of UDDI based runtime registries in the industry is extremely limited. This raises a concern as to the value of this standard.

Architectural Benefits

- Provides a standardized interface specification for service discovery
- Interoperability - platform independent

Architectural Risks

- The standard only addresses storing metadata about content. This limits its capability to a Service Registry and does not address Service Repository capabilities.

Tier Used

- Middle Tier (Integration)

General Assessment

Expected Usage:	Service discovery
Assessment Type:	New
Assessment Date:	11/3/2009
Notes:	Architectural analysis needs to be conducted to determine whether there is a need in the VA for an integrated service registry/repository. If the analysis determines value in an integrated registry/repository then the ebXML Registry standard needs be assessed as UDDI would be insufficient. This analysis also needs to include other registry/repository requirements to determine if this standard is suitable.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	UDDI is a mature industry standard. It provides a standardized interface specification for a service registry.

2.335) Universal Healthcare Identifier (UHID)

General Information

Website:	http://www.astm.org/Standards/E1714.htm
Description:	ASTM E1714: Standard Guide for Properties of a Universal Healthcare Identifier (UHID) defines a set of requirements outlining the properties required to create a UHID.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed

Introduced By: TRMSP
Vendor Name: ASTM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date

E1714-95	10/15/1995		
E1714-00	10/10/2000		
E1714-07	8/15/2007		

VA Forecast Information (10/05/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. The Benefits Segment use of the UDDI specification is currently based on version 2.0.

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.336) UNIX

General Information

Website: http://www.unix.org/

Description: ISO/IEC 9945 & IEEE 1003.1: The Single UNIX Specification is the defacto and dejure standard definition for the UNIX system application programming interfaces.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision TRMSP 4.3.2

Process:
Decision Date: 3/14/2008
Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: The Open Group

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2	3/12/1997		
3	1/30/2002		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
3	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.337) Unsolicited Email

General Information

Description: Unsolicited e-mails congest and restrict the availability of the network to work at acceptable performance levels. SPAM is defined as: to post irrelevant or inappropriate messages to one or more Usenet newsgroups, mailing lists,or other messaging system in a deliberate or accidental manner.

Decision: Approved

Decision No constraints have been specified at this time.

Constraints:

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Anti-SPAM Software Deployment		All E-mail servers shall employ anti-SPAM software
Anti-SPAM Software Updates		SPAM detection signatures shall be downloaded and installed at least monthly.
Anti-SPAM Software Configuration		Anti-SPAM software shall be configured to run in a background mode.
Procedures		Procedures shall be implemented to: • Scal all emails upon access • Scall all emails before they are transmitted to another machine • Scan all emails incoming to the domain

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Outgoing E-mail Scanning	E-mails should be SPAM scanned before they are delivered to outgoing e-mail. A record of the time and date of the scan as well as the tool used should be included inthe body of the e-mail.
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) ACT

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.338) User Authentication and Authorization

General Information

Website: http://www.astm.org/Standards/E1985.htm

Description: ASTM E1985: Standard Guide for User Authentication and Authorization

- covers mechanisms that may be used to authenticate healthcare information (both administrative and clinical) users to computer systems, as well as mechanisms to authorize particular actions by users.
- addresses both centralized and distributed environments, by defining the requirements that a single system shall meet and the kinds of information which shall be transmitted between systems to provide distributed authentication and authorization services.
- addresses the technical specifications for how to perform user authentication and authorization. The actual definition of who can access what is based on organizational policy.

Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ASTM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
98	1/1/1998		
98(2005)	1/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
98(2005)	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.339) User Datagram Protocol (UDP)

General Information

Website: http://tools.ietf.org/html/rfc768

Description: The User Datagram Protocol (UDP) is one of the core members of the Internet Protocol Suite, the set of network protocols used for the Internet. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without requiring prior communications to set up special transmission channels or data paths.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 768	8/28/1980		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 768	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.340) vConverter

General Information

Website: http://www.vizioncore.com/products/vConverter/index.php

Description: vConverter provides numerous features for effective ongoing disaster recovery in existing physical environments; vConverter generates virtual backups for physical servers; vConverter's Continuous Protection Mode regularly updates these virtual backups with changes occurring on the physical server; vConverter ensures that a "virtual standby system" that is up to date and can be immediately utilized in the event of physical server problems or outages.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: CDCO Supported Architecture Components

Vendor Name: Quest Software

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Business Logic	891: Platform Dependent Technologies

Operating Systems Supported

- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.0	12/10/2007		
4.0	11/5/2008		
4.1	2/18/2009		
4.2	7/9/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
4.0	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.341) Velocity

General Information

Website:	http://velocity.apache.org/
Description:	Velocity is a Java based templating framework. The framework provides a set of tools and a markup language for defining templates and an engine that uses the templates to generate content.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v3.2
Decision Date:	8/19/2009
Current Status:	Analysis Completed
Introduced By:	ARB
Vendor Name:	ASF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code

Component Framework	User Presentation/Interface	888: Content Rendering

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Apache Commons - ***(required libraries)***
- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.3	11/1/2005		
1.4	7/1/2006		
1.5	3/13/2007		
1.6	12/1/2008		
1.6.1	12/15/2008		
1.6.2	3/18/2009		

VA Forecast Information (06/22/2009)

The VA Forecast offers the current and future VA IT position regarding different

releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.6.1	None	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
1.6.2	None	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:	The Velocity Engine is the primary consideration in this forecast.											

General Analysis

Adoption Benefits

- Velocity template approach allows for the automation of content rendering.

Adoption Risks

- None significant.

Architectural Benefits

- An attractive alternative to Java Server Pages when the content is static, template based.

Architectural Risks

- Developers may be tempted to move business logic into the presentation layer with Velocity.

General Assessment

Expected Usage:	An alternative to Java Server Pages when a template-driven approach to HTML generation is appropriate.
Assessment Type:	New
Assessment Date:	6/22/2009

Notes:	The scope of this assessment covers the Velocity Engine and Velocity Tools.
Recommendation:	Approve
Recommendation Constraints:	None
Recommendation Justification:	Velocity has been used by Pharmacy Re-Engineering (with a waiver) for several years without issue. Velocity is an attractive alternative to Java Server Pages for some solution architectures.

2.342) Vergence Context Manager

General Information

Website:	http://www.sentillion.com/solutions/clinical-workstations.html
Description:	Vergence provides fully integrated capabilities for single patient selection. Each time the caregiver selects a new patient, all of the applications that the caregiver is using are automatically tuned to that same patient. Patient information can be reviewed and updated using each application's native capabilities, providing comprehensive and flexible access to the applications. Vergence provides a uniform set of authentication and application launching controls. The configuration of these controls can be centrally defined according to individual roles, individual desktops, groups of desktops, or enterprise-wide policies. Caregivers can use workstations throughout the enterprise in a manner that is familiar and consistent.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	Sentillion

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Requirements	860: Authentication / Single Sign-on

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (01/09/2008)

The VA Forecast offers the current and future VA IT position regarding different

releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**

VA forecast information is not available for this entry.

Forecast Note:	

General Analysis

Architectural Benefits

- The HeV architecture implements an array of highly specialized applications which comprise its presentation layer. The HeV architecture prescribes CCOW as the standardized mechanism for assuring consistent patient context across this presentation layer, an essential element for patient safety.

Architectural Risks

- Lack of documented platform support.
- Lack of documented dependencies

EA Requirement

- ENTR 1481 Clinical applications shall employ Clinical Context Object Manager for Single Sign On (SSO) support and context switching among supported applications.
- ENTR 981 Applications which identify patient shall share patient context via the HL7 Clinical Context Object Workgroup (CCOW) Specification.

General Assessment

Expected Usage: The Sentillion Vergence Context Manager clearly supports the requirements set forth in ENTR1481 to assure that context management and the user sign on are aligned. However, the product's limited public documentation does describe support for HL-7 CCOW, as specified in ENTR 981.

Assessment Type: Refresh

Assessment Date:	2/12/2009
Notes:	Very limited information is publicly available on this tool. This lack of detailed information is reflected in the limited analysis of this tool.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Recommend approval as this tool is architecturally relevant to the stated requirements, and it is currently successfully implemented in the HeV infrastructure.

2.343) Veritas Storage Foundation

General Information

Website:	http://www.symantec.com/business/storage-foundation
Description:	Veritas Storage Foundation is an online storage management solution. It allows centralized management of diverse applications, servers and storage.
Decision:	Approved
Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	Symantec

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Business Logic	890: Platform Independent Technologies

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
4.1	4/15/2005		
5.0	6/23/2006		
5.1	12/7/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
5.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.344) VHIM

General Information

Website:

Description: The Veterans Health Administration (VHA) Health Information Model (VHIM) provides an authoritative semantic and structural enterprise-level reference information model. The VHIM is realized as a Unified Modeling Language (UML) model with a collection of class diagrams serving as viewpoints into clinical domains. It classifies and represents data elements, including their relationships and constraints. Although VHIM classes and attributes are mapped to the HL7 Reference Information Model (RIM) and HL7 3.0 vocabulary domains, VHIM can be used with other standards such as ANSI X12, CHI, NCPDP, LOINC and HL7 2.5.1. The VHIM extends VA information models such as the VA Enterprise Architecture Corporate Information Model (CIM) to meet VHA-specific requirements and provide a shared, consistent representation of

data and a foundation from which more detailed and finer-grained models are derived. All public data viewable from HeV services will be represented within the VHIM.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: ARB

Decision Process: TRM v2

Decision Date: 9/17/2008

Current Status: Analysis Completed

Introduced By: TRM Team

Vendor Name: N/A

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interface	901: Service Description / Interface

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2009 R1	12/29/2008		
2011 R2 (est)	3/1/2011		
2011 R3 (est)	6/1/2011		
2011 R4 (est)	9/1/2001		
2009 R2 (est)	3/30/2009		
2009 R3 (est)	6/1/2009		
2009 R4 (est)	9/1/2009		
2010 R1 (est)	12/1/2009		
2010 R2 (est)	3/1/2009		
2010 R3 (est)	6/1/2010		
2010 R4 (est)	9/1/2010		
2011 R1 (est)	12/1/2010		

VA Forecast Information (02/03/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
200	Suppor	Suppor	Suppor	Suppor	Suppor	Suppor	Suppor	Suppor	Supp	Supp	Supp	Supp

9 R1	ted	ted	ted	ted	ted	ted	ted	ted	orted	orted	orted	orted
2010 R1 (est)	None	None	None	None	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
2011 R1 (est)	None	None	None	None	None	None	None	None	Supported	Supported	Supported	Supported

Forecast Note:	The VHIM is not a tool that is installed. It is an information model to be used in implementing applications. The forecast reflects when updates are available and cannot reflect when the guidelines will be applied by development teams.

General Analysis

Architectural Benefits

- ENTR 521 (Inactive) and 1529 specify the need for the VHIM to provide an ontology to unify the informational needs of all HeV applications. This provides stability, assures interoperability and is the framework for fulfilling informational integrity expectations for HeV data across the lengthy retention period for clinical information.
- As ENTR 665 and 666 (now marked as "inactive") describe, the VHIM provides a consistent and durable interpretation, representation, and description of the data in HeV which is essential to assure interoperability and efficient message handling across HeV components.

Architectural Risks

- Complexity - The VHIM faces an extraordinary level of complexity in the HeV architecture as it requires a concurrent and very highly detailed understanding of the data requirements from every HeV domain.
- Deviation from Standards – Ambiguity and conflicts can exist between standards requiring decisions. The result is that the VA may need to make choices that create deviations from one standard or another.
- Dependency on Standards - Continual improvements in standards upon which VHIM is based necessitates continual refinement of the VHIM to assure the implementation of industry best practices and interoperability with external partners.
- Dependency on Standards - Continual improvements in HL7, the semantic basis of VHIM, as well as other standards necessitates continual refinement of the VHIM to assure the implementation of industry best practices and interoperability with external partners.

EA Requirement

- ENTR 521 (Inactive) - The VHA Health Information Model (VHIM) shall be used as the primary source of information content and semantics.
- ENTR 1529 - All applications and services shall use the VHA Health Information Model (VHIM) as the authoritative source for semantics and information structure.
- ENTR 665 (Inactive) - HDR-N and HDR-L shall be consistent with the content and semantics defined by the VHIM/RIM.
- ENTR 1105 (Inactive) - Clinical Data Service (CDS) shall return data in one standard - the VHA Health Information Model (VHIM) conformant payload, utilizing the VHIM templates.
- ENTR 666 (Inactive) - Data shared between applications/services shall be represented in the VHIM.

Standards Traceability

- UML 2.0
- HL7
- ANSI X12
- CHI
- NCPDP
- LOINC

Tool Usage

- Runtime - Embedded
- Development

General Assessment

Expected Usage:	VHIM standardizes the representation of data and its relationships allowing interoperability of data amongst applications internal and external to HeV.
Assessment Type:	Refresh
Assessment Date:	2/3/2009
Notes:	The technology described by this assessment can be used both throughout the enterprise and to influence the evaluation of other tools. The VHIM is not a commercial tool but is a standard that is developed in-house and supports the current architectural direction. The technology described by this assessment can be used both throughout the enterprise and to influence the evaluation of other tools. Discrepancies identified amongst the standards that VHIM interprets must be resolved in close coordination with the Data Standardization team and the decisions

	documented. The VHIM actually has two product streams: VHIM version 2.x is in maintenance mode (no changes have been made in over a year) and is being used by FHIE/BHIE and CHDR. VHIM version 3.x is the basis for active development and is to be used by all HealtheVet projects. HDR/CDS are early adopters. The VHIM is released every quarter and named by the fiscal year and quarter. A Release Objective Document is released fifteen days into a ninety day release cycle and VHIM is released to the VA SharePoint and ClearCase.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	This tool is architecturally relevant to the stated requirements, and it is currently successfully implemented in the HeV infrastructure.

2.345) Video Codec for Audiovisual Services

General Information

Website:	http://www.itu.int/itu-t/recommendations/index.aspx?ser=H
Description:	ITU-T H.261: Video Codec for Audiovisual Services at p x 64 kbit/s describes the video coding and decoding methods for the moving picture component of audiovisual services at the rates of p x 64 kbit/s, where p is in the range 1 to 30.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3	3/12/1993		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on

the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
3	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.346) Virtual Bridged Local Area Networks (VLAN)

General Information

Website: https://sbwsweb.ieee.org/ecustomercme_enu/start.swe?SWENeedContext=false&SWECmd=GotoPageTab&W=t&SWEC=3&SWEScrnCap=Standards&SWEBID=-1&SWETS=1270586674437&SWEScreen=Catalog_Standards_Screen_IEEE&SWEHo=sbwsweb.ieee.org&SWETS=1270586678508&SWEC=3

Description: IEEE 802.1Q: Virtual Bridged Local Area Networks (VLAN) specifies how the MAC Service is supported by Virtual Bridged Local Area Networks, the principles of operation of those networks, and the operation of VLAN-aware Bridges, including management, protocols, and algorithms.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision TRMSP 4.3.2

Process:
Decision Date: 3/14/2008
Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: IEEE

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	Campus Area Network (CAN)*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1998	1/1/1998		
2005	1/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2005	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.347) VLAN Trunking Protocol (VTP)

General Information

Website: http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094c52.shtml

Description: VLAN Trunking Protocol (VTP) is a Cisco proprietary Layer 2 messaging protocol that manages the addition, deletion, and renaming of Virtual Local Area Networks (VLAN) on a network-wide basis.

Decision: Approved

Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	Cisco

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1			
2			
3			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.348) VM Performance Toolkit

General Information

Website: http://www.vm.ibm.com/related/perfkit/

Description: The Performance Toolkit for VM provides enhanced capabilities for a z/VM systems programmer, system operator, or performance analyst to monitor and report performance data.

Decision: Approved

Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	866: Dependent Platform

Operating Systems Supported

- z/VM

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	Refer to z/VM for release and VA Forecast information

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.349) VMware Site Recovery Manager

General Information

Website: http://www.vmware.com/products/site-recovery-manager/

Description: VMware Site Recovery Manager provides automated recovery process capabilities.

Decision: Approved

Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	VMware

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- VMware vSphere - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	6/16/2008		
4.0	10/5/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.0	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.350) VMware vCenter CapcityIQ

General Information

Website: http://www.vmware.com/products/vcenter-capacityiq/

Description:	VMware vCenter CapcityIQ provides capacity management capabilities for virtualized datacenter or desktop environments.
Decision:	Approved
Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	VMware

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- VMware vSphere - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	10/19/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.351) VMware vCenter Chargeback

General Information

Website: http://www.vmware.com/products/vcenter-chargeback/

Description:	VMware vCenter Chargeback provides cost measurement, analysis and reporting capabilities of the virtual infrastructure.
Decision:	Approved
Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	VMware

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- VMware vSphere - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	7/13/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.0	None	None	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.352) VMware vCenter Lab Manager

General Information

Website: http://www.vmware.com/products/labmanager/

Description: VMware vCenter Lab Manager provides on-demand access and automated management of the private cloud for development and test environments.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: CDCO Supported Architecture Components

Vendor Name: VMware

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- VMware vSphere - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2.5	7/9/2007		
3.0	9/12/2008		
4.0	12/10/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
3.0	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.353) VMware vCenter Server Heartbeat

General Information

Website:	http://www.vmware.com/products/vcenter-server-heartbeat/
Description:	VMware vCenter Server Heartbeat detects standard VMware vCenter Server components upon installation, providing instant monitoring and protection.
Decision:	Approved
Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	VMware

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- VMware vSphere - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.5	12/31/2007		
4.0	5/21/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
3.5	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.354) VMware vSphere

General Information

Website: http://www.vmware.com/products/vsphere/

Description: VMware vSphere, formerly known as VMware Infrastructure, provides management capability for large pools of virtualized computing infrastructure, including software and hardware.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: CDCO Supported Architecture Components

Vendor Name: VMware

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2.0	1/24/2008		
2.1	5/7/2008		
3.0	1/29/2009		
3.1	9/4/2009		
4.0	2/18/2010		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be

supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
3.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.355) VPN Services

General Information

Description: Virtual Private Network (VPN) is a service that allows authorized users to access a protected network from an untrusted network.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
RAS		The use of RAS is no longer the preferred method of

		accessing protected VA infrastructure or assets. VA approved VPN services are the preferred access method for authorized users of the VA network who must access protected assets from outside the One-VA Network.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
IETF RFC 2547	Border Gateway Protocol (BGP)/Multiprotocol Label Switching (MPLS) VPNs
IETF RFC 2917	A Core MPLS IP VPN Architecture

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.356) vRanger Pro

General Information

Website: http://www.vizioncore.com/products/vRangerPro/

Description:	vRanger Pro is a virtual backup and recovery solution.
Decision:	Approved
Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	Quest Software

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Business Logic	891: Platform Dependent Technologies

Operating Systems Supported

- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- SQL Server related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.0	1/19/2007		
3.2	9/26/2007		
3.3	6/23/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
3.2	None	None	None	None	None	None	None	None	None	None	None	None
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.357) Warehouse Services

General Information

Description: Warehouse services are a subject-oriented, integrated, time-variant, non-volatile collection of structured and non-structured data used to support the strategicdecision-making process for the enterprise. It is the central point of data integration for business intelligence delivering a common view of enterprise data.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Database/Storage	Warehouse Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.358) Web Services Description Language (WSDL)

General Information

Website:	http://www.w3.org/TR/
Description:	The Web Services Description Language (WSDL) is an XML-based language that provides a specification for describing Web services. WSDL defines the logical and physical interface of a service: what the service does and how one can access it. The WSDL defines services as collections of network endpoints in an XML format. A client program connecting to a web service can read the WSDL to determine what functions are available at another endpoint. The client can then use SOAP (or some other protocol) to call one of the functions listed in the WSDL.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	TRM Team
Vendor Name:	W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Core Langage	This specification defines the core language which can be used to describe Web services based on an abstract model of what the service offers. It also defines the conformance criteria for documents in this language.
Adjuncts	This specification specifies predefined extensions for use in WSDL 2.0: Message exchange patterns, Operation safety, Operation styles, and Binding extensions for SOAP and HTTP.
Primer	This primer is a starting point toward the use of WSDL.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interface	901: Service Description / Interface

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- WS-I Basic Profile - Standard
- Extensible Markup Language (XML) - Standard
- XML-Infoset - Standard
- XML Namespaces (XML-NS) - Standard
- XML Schema - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	9/1/2000		
1.1	3/15/2001		
1.2	7/9/2002		
2.0	6/26/2007		

VA Forecast Information (09/10/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.2	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
2.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment use of the WSDL specification is currently based on version 1.1

General Analysis

Architectural Area

- Application
- Integration

Architectural Benefits

- Decoupling: A Service Consumer does not need to know anything about how the service is implemented. All the information required to use the service is

contained in the contract (WSDL description of the Service). This separation of interface from implementation is at the heart of SOA.
- Interoperability: Service requests from any platform can read the WSDL, inspect the API and based on that inspection make calls to the described Service.
- Easy of development: All SOA-enabled IDEs can deal with WSDL, and generate a proxy class for the desired programming language (.NET, C#, VB, Java, etc.).
- Validation: While building request and response messages around XML schemas, WSDL can provide validation that the incoming message conforms to the schema.

Architectural Risks

- None significant.

EA Requirement

- ENTR 798 (Inactive) - VA/DoD Goal 4 - Integrated Information Sharing - Enable the efficient sharing of beneficiary data, medical records, and other information through secure and interoperable information management systems.
- ENTR 1074 - Implement a One VA information technology framework that supports the integration of information across business lines and that provides a source of consistent, reliable, accurate, and secure information to veterans and their families, employees, and stakeholders (Enabling Objective E-3).
- ENTR 821 (Inactive) - VHA Enabling Objective 18 - Develop innovative approaches to the design and evaluation of health care delivery systems.
- ENTR 794 (Inactive) - VHA Objective 3 - Optimize the use of health care information and technology for the benefit of the veteran.

Tier Used

- Integration Tier

Tool Usage

- Runtime - Embedded
- Development

General Assessment

Expected Usage:	WSDL is the specification for defining a web service description. In the SOA framework, WSDL can be an effective service contract between a provider and a consumer.
Assessment Type:	Standard
Assessment	9/16/2008

Date:	
Notes:	
Recommendation:	N/A
Recommendation Constraints:	
Recommendation Justification:	

2.359) WebLogic Integration

General Information

Website:	http://www.oracle.com/technology/products/weblogic/integration/index.html
Description:	WebLogic Integration adds Business Process Execution Language (BPEL) support into the WebLogic Workshop development environment. This Java development tool provides the functionality to: define business processes, use web services, access Java EE for specialized application logic, and to use WebLogic Portal resources to create user interaction with business process.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v3.1
Decision Date:	5/13/2009
Current Status:	Introduced
Introduced By:	Extended Tool List (ETL)
Vendor Name:	Oracle

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	896: Enterprise Application Integration

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- WebLogic Server - ***(required libraries)***
- JRE - Sun - ***(required for some configurations)***

Comparable Technologies/Standards:

- Eclipse

Companion Technologies/Standards:

- WebLogic Portal related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
7.0	6/29/2002	4/15/2009	4/15/2011
8.1	7/15/2003	9/30/2009	9/30/2011
9.2	11/28/2006	11/30/2011	11/30/2013
10.2	2/15/2008	3/31/2013	3/31/2015
10.3	9/1/2008	3/31/2013	3/31/2015
11 (est)	9/1/2009		

VA Forecast Information (03/16/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
8.1	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
9.2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated
10.3	None	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Architectural Area

- Application

Architectural Benefits

- The vendor appears to be committed to Java EE standards and provides commercial support.
- WebLogic Integration provides an OS independent mechanism to model and integrate business processes into WebLogic Portal applications.

Architectural Risks

- Oracle has placed WebLogic Integration in the "continue and converge" classification, and has announced plans that Integration will be subjugated into Oracle's BPEL PM product. However, Oracle has stated that it will continue to support WebLogic Integration into the next nine years. There is a risk that Oracle may change from their announced position and commitment of support for Workshop for WebLogic into the next nine years (until 2017).

Tool Type

- Tool

Tool Usage

- Development

General Assessment

Expected Usage:	Model and integrate business processes into WebLogic Portal applications. BPEL import and export.
Assessment Type:	New
Assessment Date:	3/16/2009
Notes:	At some point in the future, WebLogic Portal products will need to migrate to Oracle's WebCenter Framework, or some other technical foundation for portal projects. The situation will need to be re-evaluated annually, at a minimum. Project teams planning to deploy applications on WebLogic Portal need to address licensing early in project planning.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Oracle's product roadmap calls for the BEA Workshop components to be integrated in Oracle's Enterprise Eclipse Pack. However, in the short-term (until 2010), Portal development teams will realize higher productivity using Workshop for WebLogic compared to generic Eclipse or IBM Rational environments.

2.360) WebLogic Portal

General Information

Website:	http://www.oracle.com/products/middleware/user-interaction/weblogic-portal.html
Description:	BEA WebLogic Portal is now known as WebLogic Portal. WebLogic Portal is a well-known, widely-used, Java-based portal product and a portal framework. The WebLogic Portal product is out-of-the-box software that aggregates information, content, applications, business processes and knowledge assets into a personalized display. The

WebLogic Portal framework is the portal product in kit form, providing a set of tools to extensively build and customize a portal with specialized functionality. The WebLogic Portal framework comes packaged with an Eclipse-based integrated development environment (IDE) to assemble and extend the capabilities of the portal using the provided API and tools. The paired IDE is known as Oracle Workshop for WebLogic (formerly WorkSpace Studio).

WebLogic Portal offers excellent support for industry standards, enterprise-class portal federation, publication, and syndication capabilities including bidirectional integration with other portals and Web applications. MyHealtheVet and the Clinical Information Support System (CISS) are deployed with WebLogic Portal.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: ARB

Decision Process: TRM v3.1

Decision Date: 5/13/2009

Current Status: Introduced

Introduced By: Extended Tool List (ETL)

Vendor Name: Oracle

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	895: Middleware

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- WebLogic Server - ***(required libraries)***
- WebLogic Integration - ***(required for some configurations)***
- Workshop for WebLogic - ***(required for some configurations)***
- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
7.0	6/29/2002	4/15/2009	4/15/2011
8.1	7/15/2003	9/30/2009	9/30/2011
9.2	11/28/2006	11/30/2011	11/30/2013
10.2	2/15/2008	3/31/2013	3/31/2015
10.3	9/1/2008	3/31/2013	3/31/2015
11 (est)	9/1/2009		

VA Forecast Information (02/13/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
9.2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated
10.3	None	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Architectural Area

- Application
- Integration

Architectural Benefits

- The vendor appears to be committed to Java EE standards and provides commercial support.
- WebLogic Portal has been successfully deployed in the VA infrastructure (My HEV).
- WebLogic Portal provides an OS independent mechanism for developing-deploying Portal applications.

Architectural Risks

- Oracle may change from their announced position and commitment of support for WebLogic Portal into the next nine years (until 2017).
- Oracle has placed WebLogic Portal in the "continue and converge" classification, and has announced plans to integrate WebLogic Portal components into Oracle WebCenter. However, Oracle has stated that it will continue to support WebLogic Portal for the next nine years.

EA Requirement

- Complies with current Enterprise Architecture direction as an SOA-compliant industry standard Portal product-framework.

Standards Traceability

- Java Specification Request 286
- Web Services for Remote Portlets (WSRP)

- Java Specification Request 188
- Java Specification Request 168
- Java Specification Request 170

Tier Used

- Middle Tier (Infrastructure)
- Client Tier
- Presentation Tier (Web)
- Middle-Tier (Business)
- Middle Tier (Integration)

Tool Type

- Platform

Tool Usage

- Development
- Management/Collaboration
- Runtime

General Assessment

Expected Usage:	
Assessment Type:	Re-Assess
Assessment Date:	2/6/2009
Notes:	At some point in the future, WebLogic Portal products will need to migrate to Oracle's WebCenter Framework, or some other technical foundation for portal projects. The situation will need to be re-evaluated annually, at a minimum. Project teams planning to deploy applications on WebLogic Portal need to address licensing early in project planning.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	WebLogic Portal is already embedded in the VA (My HealtheVet has been deployed with WebLogic Portal since 2007). As WebLogic Server is also widely deployed in the VA, WebLogic

Portal should be the preferred portal product for the next 2-years. Oracle's position on WebLogic Portal must be monitored.

2.361) WebLogic Scripting Tool

General Information

Website:	http://download.oracle.com/docs/cd/E13222_01/wls/docs92/config_scripting/using_WLST.html
Description:	Command-line and Eclipse plug-in scripting interface for WebLogic administration.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v3.2
Decision Date:	8/19/2009
Current Status:	Assessment Complete
Introduced By:	ARB
Vendor Name:	Oracle

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	867: Integrated Development Environments (IDE)

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- WebLogic Server - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (06/11/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	This tool is part of the WebLogic Server software suite. Please refer to the Weblogic Server entry for the VA Forecast.

General Analysis

Adoption Benefits

- The WebLogic Scripting Tool provides automation for WebLogic Server deployments.

Adoption Risks

- None significant.

Architectural Benefits

- This tool is consistent with the current business tier architecture.

Architectural Risks

- None significant.

General Assessment

Expected Usage:	Create, configure, and manage WebLogic domains.
Assessment Type:	New
Assessment Date:	6/11/2009
Notes:	The WLST is based on the Java scripting interpreter, Jython.
Recommendation:	Approve
Recommendation Constraints:	Use of WLST must be tightly coordinated with EIE.
Recommendation Justification:	WLST has been included with WebLogic Server since version 9.0. EIE encourages the use of WLST to automate routine maintenance tasks.

2.362) WebLogic Server

General Information

Website:	http://www.oracle.com/appserver/weblogic/weblogic-suite.html

Description:	WebLogic Enterprise is now WebLogic Server, a foundational element of the WebLogic application platform. The WebLogic Service is a Java Enterprise Edition application server platform, designed to host distributed applications written using Java and the Java Enterprise Edition frameworks. The WebLogic Platform also includes Integration, Portal, Blended Frameworks and Workshop IDE.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	Oracle

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	873: Application Servers

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required for some configurations)***
- Web Services Description Language (WSDL) - ***(required for some configurations)***
- Simple Object Access Protocol (SOAP) - ***(required for some configurations)***
- WS-Security - ***(required for some configurations)***
- Extensible Markup Language (XML) - ***(required for some configurations)***
- Universal Description, Discovery, and Integration (UDDI) - ***(required for some configurations)***
- WS-I Basic Profile - ***(required for some configurations)***
- WS-Reliable Messaging - ***(required for some configurations)***
- XSL Transformations (XSLT) - ***(required for some configurations)***
- XQuery - ***(required for some configurations)***
- Java EE - ***(required for some configurations)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
7.0	6/29/2002	4/15/2009	4/15/2011
8.1	7/15/2003	9/30/2009	9/30/2011
9.2	11/28/2006	11/30/2011	11/30/2013
10.2	2/15/2008	3/31/2013	3/31/2015
10.3	9/1/2008	3/31/2013	3/31/2015
11g (10.3.1)	7/1/2009		

VA Forecast Information (09/30/2009)

The VA Forecast offers the current and future VA IT position regarding different

releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
8.1	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
9.2	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
10.3	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
11g (10.3.1)	None	None	None	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment development and deployment of WebLogic Server is currently based on version 10.3.											

General Analysis

Architectural Area

- Application
- Integration

Architectural Benefits

- The WebLogic application server provides a platform independent mechanism for developing, deploying and running HeV applications.
- The vendor appears to be committed to Java EE standards and provides commercial support.
- WebLogic Server is commercially available and Java EE compliant.

Architectural Risks

- The Oracle purchase of BEA creates unknowns about how WebLogic will fit-in with the Oracle fusion middleware.

EA Requirement

- Deploy an SOA compliant Java EE application server.

Standards Traceability

- JAX-WS 2.0
- JAXB 2.0
- Java EE 5
- EJB 3.0
- Java Persistence API (JPA)

Tier Used

- Middle Tier (Infrastructure)
- Client Tier
- Presentation Tier (Web)
- Middle Tier (Business)
- Middle Tier (Integration)

Tool Type

- Platform

Tool Usage

- Development
- Management/Collaboration
- Runtime

General Assessment

Expected Usage:	To provide a Java EE compliant application server on which to deploy and run Java EE based applications.
Assessment Type:	Refresh
Assessment Date:	9/5/2008
Notes:	WebLogic Server is one element of the WebLogic Platform that includes: Portal, Integration, Workshop IDE, JRockit, and other technologies. Only WebLogic server is in the scope of this assessment.
Recommendation:	Approve

Recommendation Constraints:	
Recommendation Justification:	Continue with WebLogic Server.

2.363) Wide Area Network (WAN)

General Information

Refer to document:	VA_Enterprise_IT_Infrastructure_Standard_WAN_1_0.pdf
Description:	This standards document lists the acceptable and recommended specifications for Wide Area Network. Sections include standard specifications for subject components, decisions supporting the standard specifications, guidelines or recommendations for implementing the standard specifications, and supplemental factors to consider when evaluating subject components. Other supplementary documents will provide guidance on procuring components that meet the standard specifications, guidance on integrating them with existing components, and explanation of how the subject components fit into the VA Architecture. This standard includes the following: Class A Router (Chassis; Packet Processor; Interface Cards; Operating System; WAN Encryption; Platform Supportability; Platform Maturity); Class B Router (Chassis; Packet Processor; Interface Cards; Operating System; WAN Encryption; Platform Supportability; Platform Maturity); Wide Area Network (Metro Data Center To Backbone; Metro Data Center to Region WAN; Medical Center to Region WAN; Medical Center Branch Office to Region WAN); WAN Encryption (Data Center; Medical Center); WAN Acceleration (Data Center; Medical Center).
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EIE CTO
Decision Process:	TAR-TAS
Decision Date:	11/30/2009

Current Status: Analysis Completed
Introduced By: OPS/EIE

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	880: Wide Area Networks (WAN)

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (09/30/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment development and deployment of WebLogic Server is currently based on version 10.3.

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.364) Wi-Fi Protected Access (WPA)

General Information

Website:	http://www.wi-fi.org/knowledge_center/wpa2
Description:	Wi-Fi Protected Access (WPA) provides network administrators with a high level of assurance that only authorized users can access the network. Based on the ratified IEEE 802.11i standard, WPA provides government grade security by implementing the National Institute of Standards and Technology NIST FIPS 140-2 compliant AES encryption algorithm.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.

Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	Wi-Fi Alliance

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
WPA	4/1/2003		
WPA2	9/2/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
WPA 2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.365) Wily Introscope

General Information

Website: http://www.ca.com/us/application-management.aspx

Description: Wily Introscope is an application management product that allows monitoring, proactive detection, triage and diagnosis of performance

problems in complex, composite and Web application environments.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: CDCO Supported Architecture Components

Vendor Name: CA

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Enterprise Manager	The Enterprise Manager (EM) acts as the central repository for all Introscope performance data and metrics collected in an application environment. The EM processes performance data and makes it available to users for production monitoring and diagnosis.
WebView	Introscope WebView presents Web-based graphical UI to display Introscope performance data. Introscope's customizable dashboards and Explorer tree views for authorized users run in a browser interface, so that critical information can be viewed by those who need it anytime, anywhere. Note that the WebView component requires the Adobe SVG Viewer browser plug-in to display performance data.
Agent	Introscope agents collect performance metrics from the various components inside the running Web application, the application server and performance and availability data from the surrounding computing environment. The agents then report these metrics to the Enterprise Manager.
Workstation	The user controls Introscope and accesses performance metrics through the Introscope Workstation. Users can set alerts for individual metrics or logical metric groups, view performance metrics, and customize views to

	represent their unique environment. The Introscope Workstation has a Swing-based UI, for onsite or in-house use only

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- BMC Performance Manager
- Foglight

Companion Technologies/Standards:

- Apache Commons related as: (Companion)
- Apache Tomcat related as: (Companion)
- JasperReports related as: (Companion)
- Log4J related as: (Companion)
- JRE - Sun related as: (Companion)
- JAXB Reference Implementation related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date

7.2			
8	6/16/2008		
8.1			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.366) Windows (Client)

General Information

Website: http://www.microsoft.com/windows/windows-xp/

Description: Microsoft's Windows XP is the principal client operating system used in HeV. Windows XP is a line of proprietary operating systems developed by Microsoft for use on general-purpose computer systems, including home and business desktops, notebook computers, and media centers. Windows XP began development in early 1999 and is the successor to both Windows 2000 and Windows Me, and is the first consumer-oriented operating system produced by Microsoft to be built on the Windows NT kernel and architecture. Windows XP was first released October 25, 2001, and an estimate of more than 400 million copies are in use, Two separate 64-bit versions of Windows XP were also released, Windows XP 64-bit Edition for IA-64 (Itanium) processors and

Windows XP Professional x64 Edition for x86-64 processors. Windows XP is known for its improved stability and efficiency over previous versions of Microsoft Windows. It presents a significantly redesigned graphical user interface, a change Microsoft promoted as more user-friendly than previous versions of Windows. New software management capabilities were introduced to avoid the DLL deployment issues that plagued older consumer versions of Windows. It is also the first version of Windows to use product activation to combat software piracy.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: ARB

Decision Process: TRM v2

Decision Date: 9/17/2008

Current Status: Analysis Completed

Introduced By: TRM Team

Vendor Name: Microsoft

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	866: Dependent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Red Hat Linux

Companion Technologies/Standards:

- Internet Information Services (IIS) related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
XP Pro	12/31/2001	4/1/2009	4/18/2014
XP Pro SP2	9/17/2004	6/13/2010	
XP Pro SP3	5/6/2008		
Vista	1/25/2007	4/13/2010	
Vista SP1	4/25/2008		
Vista SP2	5/25/2009		
Windows 7	10/22/2009		

VA Forecast Information (10/16/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
XP Pro	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated

SP2												
XP Pro SP3	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	EIE Information Bulletin for XP Pro SP 3 **The installation of Windows VistA is currently prohibited** **The installation of Windows 7 is currently prohibited -** EIE Memorandum

General Analysis

Architectural Area

- Application

Architectural Benefits

- The client operating system is a critical component of the infrastructure as it provides a standardized client platform for the deployment and execution of HeV application software. Such a standardized client platform stabilizes application development and deployment objectives, simplifies hardware management at the client level, and greatly simplifies the end user operational and training experiences.

Architectural Risks

- Security vulnerabilities - Windows operating system products have a considerable history of security vulnerabilities and breaches requiring frequent patching.
- System load concerns - OS specific, detailed capacity planning is not integrated proactively into design and development activities.
- Vendor lock in - Rich client software is designed, developed and optimized specifically for deployment on Windows. Moving those applications to another operating system in the future could require significant effort and cost.

EA Requirement

- ENTR 68 (inactive) - The entire suite of deployable software (i.e., Operating System, Database Engine, Mid-Tier, and Reports) shall be identified and documented.
- ENTR 91 - Deployment of new software and/or upgrades shall use standard tools and/or follow standard procedures established for use by the Office of Information.

Standards Traceability

- Microsoft lists standards compliance program information at: http://www.microsoft.com/about/legal/intellectualproperty/standards/default.mspx

Tier Used

- Presentation Tier (Web)
- Client Tier
- Presentation Tier (Thick)

Tool Type

- Platform

Tool Usage

- Runtime
- Development

General Assessment

Expected Usage:	The implementation of Windows (Client) and its inclusion in the TRM fulfills the objectives outlined in ENTR68 (now marked as "inactive"), and also the management standardization objectives described in ENTR91.
Assessment Type:	Refresh
Assessment Date:	2/3/2009
Notes:	As Windows XP has already been superseded by the Windows Vista product, EOL and support issues are key to the implementation of this product. Detailed statements of Microsoft support policy are available at: http://support.microsoft.com/gp/lifepolicy. Detailed support timeline information for the Windows XP product can be found at: http://support.microsoft.com/lifecycle/?LN=en-us&x=9&y=12&C2=1173.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Recommend approval as this tool is architecturally relevant to the stated requirements, and it is successfully implemented in the HeV infrastructure.

2.367) Windows (Server)

General Information

Website:	http://www.microsoft.com/windowsserver2008/en/us/default.aspx
Description:	Windows Server is a proprietary operating system developed by Microsoft for use on server computer systems.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	TRM Team
Vendor Name:	Microsoft

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	866: Dependent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- Universal Description, Discovery, and Integration (UDDI) - ***(required libraries)***

Comparable Technologies/Standards:

- Solaris
- HP-UX
- AIX
- Red Hat Linux

Companion Technologies/Standards:

- Active Directory related as: (Companion)
- Internet Information Services (IIS) related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2003	4/1/2003		4/10/2007
2003 SP1	3/1/2005		4/14/2009
2003 SP2	8/1/2007		
2008	2/28/2008		
2008 SP1	9/17/2008		
2008 SP2	5/25/2009		

VA Forecast Information (10/19/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009	CY2010	CY2011

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2003 SP2	Supported	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
2008 SP1	Planning	Evaluation	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
2008 SP2	None	None	Planning	Evaluation	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Architectural Area

- Application
- Data
- Integration

Architectural Benefits

- The operating system is a critical component of the enterprise infrastructure. Windows provides an operating systems platform which supports modular deployment which is independent of the hardware manufacturer.

Architectural Risks

- Excessive complexity - Windows is currently deployed in HealtheVet with other enterprise operating systems including AIX, RedHat, Solaris and HP-UX. The combination of operating systems significantly complicates server monitoring, application deployment, machine optimization, and capacity planning.

EA Requirement

- ENTR 68 (Inactive) - The entire suite of deployable software (i.e., Operating System, Database Engine, Mid-Tier, and Reports) shall be identified and documented.
- ENTR 91 - Deployment of new software and/or upgrades shall use standard tools and/or follow standard procedures established for use by the Office of Information.

Standards Traceability

- Microsoft lists its standards compliance program information at: http://www.microsoft.com/about/legal/intellectualproperty/standards/default.mspx

Tier Used

- Middle Tier (Integration)
- Middle Tier (Business)
- Client Tier
- Middle Tier (Infrastructure)
- Data Tier

Tool Type

- Platform

Tool Usage

- Development
- Management/Collaboration
- Runtime

General Assessment

Expected Usage:	The implementation of Windows Server operating systems and its inclusion in the TRM fulfills the objectives outlined in ENTR68 (now marked as "inactive"), and the management standardization objectives described in ENTR91.
Assessment Type:	Refresh
Assessment Date:	2/3/2009
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Recommend approval as this tool is architecturally relevant to the stated requirements, and it is currently successfully implemented in the HealtheVet infrastructure.

2.368) WinSCP

General Information

Website: http://winscp.net/eng/docs/introduction

Description:	WinSCP is an open source SFTP and FTP client for Windows. Legacy SCP protocol is also supported. WinSCP's main purpose is the safe copying of files between a local and a remote computer. WinSCP is licensed for free distribution under the GNU general public license.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v3
Decision Date:	1/7/2009
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	SourceForge

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
N/A	N/A	N/A

Operating Systems Supported

- Windows (Client)

Technologies/Standards Relationships

Runtime Dependencies:

- Windows (Client) - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.1	7/15/2003		
3.5	1/14/2004		
3.7	10/13/2004		
3.8.1	5/7/2006		
4.0.3	7/12/2007		
4.1.7	9/28/2008		
4.2 (est)	10/31/2009		

VA Forecast Information (11/10/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008				CY2009				CY2010			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
3.5	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
3.7	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
4.0.	None	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

3												
4.1.7	None	None	None	**Planning**	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
4.2 (est)	None	None	None	None	None	None	None	None	None	None	**Planning**	**Planning**
Forecast Note:												

General Analysis

Architectural Benefits

- WinSCP allows for secure data transfer using common protocols.

Architectural Risks

- None significant.

EA Requirement

- ENTR 1074 - Implement a One VA information technology framework that supports the integration of information across business lines and that provides a source of consistent, reliable, accurate, and secure information to veterans and their families, employees, and stakeholders (Enabling Objective E-3).

Standards Traceability

- FTP (File Transfer Protocol)
- SFTP (SSH File Transfer Protocol)
- SCP (Secure Copy Protocol)

Tool Type

- Open Source

Tool Usage

- Management/Collaboration

General Assessment

Expected Usage:	WinSCP is a secure file transfer client for Windows.
Assessment	New

Type:	
Assessment Date:	11/10/2008
Notes:	WinSCP is available as a plugin to FAR (File and Archive) Manager.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	WinSCP is available to project teams at no cost and allows for the secure transfer of data between computers. Note that the VA server configuration disables FTP so the use of SFTP and SCP is required.

2.369) Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY)

General Information

Website:	http://standards.ieee.org/getieee802/download/802.11-2007.pdf
Description:	IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) defines the standard for wireless local area networks (WLANS).
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IEEE

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	881: Local Area Networks (LAN)
Service Platform and Infrastructure	Hardware/Infrastructure	Campus Area Network (CAN)*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2003	1/1/2003		
2007	6/12/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2003	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.370) Wireless Mobile Voice

General Information

Description: Consists of the software and protocols used for wireless and voice enabled presentation devices.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Security of External Electronic Connections	VA Directive 6212	This document describes the minimum security requirements for Department of Veterans Affairs (VA) external electronic connections.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Web-centric	User Interfaces (UI) should be platform independent; therefore, the preferred approach to UIs on mobile devices is to use Web Client-Services via (micro) browsers.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	864: Wireless / Mobile

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

2.371) Wireless Transport Layer Security (WTLS)

General Information

Website: http://www.openmobilealliance.org/tech/affiliates/wap/wapindex.html

Description: WAP-261: Wireless Transport Layer Security Specification (WTLS) provides privacy, data integrity and authentication between two communicating applications. WTLS provides functionality similar to TLS 1.0 and incorporates new features such as datagram support, optimised handshake and dynamic key refreshing. The WTLS protocol is optimised for low-bandwidth bearer networks with relatively long latency.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: OMA

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
20010406	4/6/2001		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
20010406	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.372) Workshop for WebLogic

General Information

Website: http://www.oracle.com/technology/products/workshop/index.html

Description: Workshop for WebLogic was formerly listed on the TRM as WebLogic Workshop. The WebLogic Portal framework comes packaged with an Eclipse-based integrated development environment (IDE) to assemble and extend the capabilities of the portal using the provided API and tools. The paired IDE is now known as Oracle Workshop for WebLogic (formerly WorkSpace Studio).

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: ARB

Decision Process: TRM v3.1

Decision Date: 5/13/2009

Current Status: Analysis Completed

Introduced By: Extended Tool List (ETL)

Vendor Name: Oracle

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code

Service Platform and Infrastructure	Software Engineering	867: Integrated Development Environments (IDE)

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- WebLogic Server - ***(required libraries)***
- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- Eclipse

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
7.0	6/29/2002	4/15/2009	4/15/2011
8.1	7/15/2003	9/30/2009	9/30/2011
9.2	11/28/2006	11/30/2011	11/30/2013
10.2	2/15/2008	3/31/2013	3/31/2015
10.3	9/1/2008	3/31/2013	3/31/2015
11 (est)	9/1/2009		

VA Forecast Information (03/16/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or

production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
8.1	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
9.2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated
10.3	None	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Architectural Area

- Application

Architectural Benefits

- The vendor appears to be committed to Java EE standards and provides commercial support.
- Workshop for WebLogic has been successfully deployed in the VA infrastructure (My HEV).
- Workshop for WebLogic provides an OS independent mechanism for developing-deploying Portal applications.

Architectural Risks

- Oracle has placed Workshop for WebLogic in the "continue and converge" classification, and has announced plans that Workshop components will be integrated in Oracle's Enterprise Eclipse Pack. However, Oracle has stated that it will continue to support Workshop for WebLogic into the next nine years. There is a risk that Oracle may change from their announced position and commitment of support for Workshop for WebLogic into the next nine years (until 2017).

Tool Type

- Tool

Tool Usage

- Development

General Assessment

Expected Usage:	An integrated development environment to design-build WebLogic Portal applications.
Assessment Type:	New
Assessment Date:	3/9/2009
Notes:	At some point in the future, WebLogic Portal products will need to migrate to Oracle's WebCenter Framework, or some other technical foundation for portal projects. The situation will need to be re-evaluated annually, at a minimum. Project teams planning to deploy applications on WebLogic Portal need to address licensing early in project planning.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Oracle's product roadmap calls for the BEA Workshop components to be integrated in Oracle's Enterprise Eclipse Pack. However, in the short-term (until 2010), Portal development teams will realize higher productivity using Workshop for WebLogic compared to generic Eclipse or IBM Rational environments.

2.373) WS-Reliable Messaging

General Information

Website:	http://www.oasis-open.org/specs/#wsrx-rmv1.2
Description:	The Web Services Reliable Messaging (WS-RM) specification describes a protocol that allows messages to be transferred reliably between nodes implementing this protocol in the presence of software component, system, or network failures. The protocol is described in this specification in a transport-independent manner allowing it to be implemented using different network technologies. To support interoperable Web services, a SOAP binding is defined within this specification. The protocol defined in this specification depends upon other Web

services specifications for the identification of service endpoint addresses and policies. How these are identified and retrieved are detailed within those specifications and are out of scope for this document.

By using the XML, SOAP, and WSDL extensibility model, SOAP-based and WSDL-based specifications are designed to be composed with each other to define a rich Web services environment. As such, WS-ReliableMessaging by itself does not define all the features required for a complete messaging solution. WS-ReliableMessaging is a building block that is used in conjunction with other specifications and application-specific protocols to accommodate a wide variety of requirements and scenarios related to the operation of distributed Web services

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: Benefits Arch

Decision Process: TRM v4.1

Decision Date: 10/28/2009

Current Status: Analysis Completed

Introduced By: Benefits ASA

Vendor Name: OASIS

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- ebXML Messaging Service (ebMS)

Companion Technologies/Standards:

- Simple Object Access Protocol (SOAP) - Standard
- Web Services Description Language (WSDL) - Standard
- Extensible Markup Language (XML) - Standard
- XML Namespaces (XML-NS) - Standard
- XML Schema - Standard
- XML Path Language (XPath) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.1	1/7/2008		
1.2	9/10/2008		

VA Forecast Information (10/08/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009	CY2010	CY2011

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.1	None	None	None	Supported	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated
1.2	None	None	None	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment use of the WS-Reliable Messaging specification is currently based on version 1.1

General Analysis

Adoption Risks

- It currently has a limited industry implementation footprint.
- It is relatively new industry standard.

Architectural Benefits

- Transport independent protocol that support reliable delivery of messages.
- Supports reliable sequenced delivery of SOAP messages.

Tier Used

- Middle Tier (Infrastructure)
- Middle Tier (Integration)

General Assessment

Expected Usage:	Provide a protocol standard that allows SOAP messages to be reliably delivered between distributed applications in the presence of software component, system, or network failures.
Assessment Type:	New
Assessment Date:	11/3/2009
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation	WS-RM provides a transport independent standard which enables Web Services to transmit sequences of messages across nodes

Justification: reliably and in conformance with various rules called quality assurances.

2.374) WS-Security

General Information

Website: http://www.oasis-open.org/specs/#wssv1.1

Description: Web Services Security (WS-Security) describes enhancements to SOAP messaging to provide message integrity and confidentiality. The specified mechanisms can be used to accommodate a wide variety of security models and encryption technologies.

This specification also provides a general-purpose mechanism for associating security tokens with message content. No specific type of security token is required, the specification is designed to be extensible (i.e. support multiple security token formats).

For example, a client might provide one format for proof of identity and provide another format for proof that they have a particular business certification.

Additionally, this specification describes how to encode binary security tokens, a framework for XML-based tokens, and how to include opaque encrypted keys. It also includes extensibility mechanisms that can be used to further describe the characteristics of the tokens that are included with a message.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: Benefits Arch

Decision Process: TRM v4.1

Decision Date: 10/28/2009

Current Status: Analysis Completed

Introduced By: Benefits ASA

Vendor Name: OASIS

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	885: Supporting Security Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Simple Object Access Protocol (SOAP) - Standard
- Extensible Markup Language (XML) - Standard
- XML Schema - Standard
- XML Namespaces (XML-NS) - Standard
- XML Path Language (XPath) - Standard
- Security Assertion Markup Language (SAML) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	3/15/2004		

1.1	2/21/2006		

VA Forecast Information (10/08/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.1	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Adoption Benefits

- WS-Security is a mature and widely adopted industry standard for securing Web Services.

Architectural Benefits

- WS-Security provides support for signing and encrypting SOAP messages.
- Messages can be protected from end to end, all the way from the original consumer, across any potential intermediaries on the message's path, to the provider and back again (unlike SSL/TLS where an intermediary would need to decrypt/process/encrypt the message).
- WS-Security supports the use of security tokens for SOAP messages.
- WS-Security defines communication protocol for secure web service message exchange (confidentiality, integrity, non-repudiation).

Tier Used

- Middle Tier (Infrastructure)

General Assessment

Expected Standard communication protocol for securing Web Services.

Usage:	
Assessment Type:	New
Assessment Date:	11/3/2009
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	WS-Security is a mature, widely adopted industry standard that provides end to end security for SOAP based messaging.

2.375) X.500 The Directory

General Information

Website:	http://www.itu.int/itu-t/recommendations/index.aspx?ser=X
Description:	ITU-T X.500: The Directory introduces the concepts of the Directory and the DIB (Directory Information Base) and overviews the services and capabilities which they provide.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
4	2/2/2001		
5	8/29/2005		
6	11/13/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on

the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
5	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.376) X.509 Certificate Request Message Format (CRMF)

General Information

Website: http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

Description: The Internet X.509 Certificate Request Message Format (CRMF) is used to convey a request for a certificate to a Certification Authority (CA), possibly via a Registration Authority (RA), for the purposes of X.509 certificate production. The request will typically include a public key and associated registration information.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2511	3/1/1999		

RFC 4211	9/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
RFC 2511	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.377) X.509 PKI Representation of Key Exchange Algorithm (KEA) Keys

General Information

Website: http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

Description: The Key Exchange Algorithm (KEA) is a classified algorithm for exchanging keys. This specification profiles the format and semantics of fields in X.509 V3 certificates containing KEA keys. The specification addresses the subject PublicKeyInfo field and the keyUsage extension.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision FA

Source:	
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2528	3/1/1999		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2528	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.378) X.509 Public Key Infrastructure (PKI) Certificate and CRL Profile

General Information

Website: http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

Description: The Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile describe the X.509 certificate and X.509 CRL for use in the Internet. The X.509 certificate format is described in detail, with additional information

regarding the format and semantics of Internet name forms (e.g., IP addresses). Standard certificate extensions are described and one new Internet-specific extension is defined. A required set of certificate extensions is specified. The X.509 CRL format is described and a required extension set is defined as well. An algorithm for X.509 certificate path validation is described. Supplemental information is provided describing the format of public keys and digital signatures in X.509 certificates for common Internet public key encryption algorithms (i.e., RSA, DSA, and Diffie-Hellman).

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2459	1/1/1999		
RFC 3280	4/1/2002		
RFC 5280	5/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 3280	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.379) X.509 Public Key Infrastructure (PKI) Certificate Management Protocols

General Information

Website:	http://www.rfc-editor.org/cgi-bin/rfcsearch.pl
Description:	The Internet X.509 Public Key Infrastructure (PKI) Certificate Management Protocols define the protocol messages for all relevant aspects of certificate creation and management.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2510	3/1/1999		
RFC 4210	9/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo

2510	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.380) X.509 Public Key Infrastructure LDAP Schema

General Information

Website: http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

Description: The Internet X.509 Public Key Infrastructure LDAPv2 Schema is a minimal schema to support PKIX in an LDAPv2 environment. Only PKIX-specific components are specified. LDAP servers, acting as PKIX repositories should support the auxiliary object classes defined in this specification and integrate this schema specification with the generic and other application-specific schemas as appropriate, depending on the services to be supplied by that server.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2587	6/1/1999		
RFC 4523	6/1/2006		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is

considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2587	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.381) X.509 Public Key Infrastructure Online Certificate Status Protocol (OCSP)

General Information

Website: http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

Description: The Internet X.509 Public Key Infrastructure Online Certificate Status Protocol (OCSP) specifies a protocol useful in determining the current status of a digital certificate without requiring Certificate Revocation Lists (CRLs).

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2560	6/1/1999		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or

production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2560	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.382) X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP

General Information

Website: http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

Description: Internet X.509 Public Key Infrastructure (PKI) Operational Protocols: FTP and HTTP specifies the conventions for using the File Transfer Protocol (FTP) and the Hypertext Transfer Protocol (HTTP) to obtain certificates and Certificate Revocation Lists (CRLs) from PKI repositories.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2585	5/1/1999		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on

the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2585	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.383) X.509 Public Key Infrastructure Operational Protocols: LDAP

General Information

Website: http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

Description: The Internet X.509 Public Key Infrastructure Operational Protocols: LDAP - addresses requirements to provide access to Public Key Infrastructure (PKI) repositories for the purposes of retrieving PKI information and managing that same information. The mechanism is based on the Lightweight Directory Access Protocol (LDAP) defining a profile of that protocol for use within the IPKI and updates encodings for certificates and revocation lists.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0 (RFC 2559)	4/1/1999		

2.0 (RFC 3494)	3/1/2003		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.0 (RFC 2559)	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.384) X.509 Public-Key and Attribute Certificate Frameworks

General Information

Website: http://www.iso.org/iso/catalogue_detail.htm?csnumber=34551

Description: ISO/IEC 9594-8, ITU-T X.509, & IETF RFC 3647: Public-Key and Attribute Certificate Frameworks defines a framework for public-key certificates and attribute certificates. These frameworks may be used by other standards bodies to profile their application to Public Key Infrastructures (PKI) and Privilege Management Infrastructures (PMI). Also, this standard defines a framework for the provision of authentication services by Directory to its users. It describes two levels of authentication: simple authentication, using a password as a verification of claimed identity; and strong authentication, involving credentials formed using cryptographic techniques. While simple

authentication offers some limited protection against unauthorized access, only strong authentication should be used as the basis for providing secure services.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
4	3/31/2001		
5	1/1/2005		
5.1	1/13/2007		
5.2	11/13/2008		
6	11/13/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
5.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.385) XDoclet

General Information

Website:	http://xdoclet.sourceforge.net/xdoclet/index.html
Description:	XDoclet is open source software that extracts text annotations from source code to generate other artifacts such as XML descriptors or additional code remnants. XDoclet has been superannuated by the annotation support in Java SE, but the framework still has utility.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	CodeHaus

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	868: Software Configuration Management

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris

- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- ANT - ***(required libraries)***

Comparable Technologies/Standards:

- Java SE

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.2.1	10/23/2004		
1.2.3	4/15/2005		

VA Forecast Information (01/12/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.2.3	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Architectural Area

- Integration
- Data
- Application

Architectural Benefits

- Use of the XDoclet artifact generator can promote standardization, and therefore, application portability.

Architectural Risks

- Continued use of XDoclet may lead to the introduction of another container for dependency injection (Pico) that would be duplicative to the widely deployed Spring container. Introduction of additional containers adds to application complexity and reduces portability.

Tool Type

- Framework

Tool Usage

- Development

General Assessment

Expected Usage:	Provide general purpose framework for code generation through a combination of annotations and configuration.
Assessment Type:	Refresh
Assessment Date:	1/13/2009
Notes:	Java SE 5 and Java EE 5 introduced the functionality formerly found only in XDoclet; the original open source project has had minimal activity since 2005. There is an XDoclet2 implementation, but it uses a completely different architecture that requires the introduction of the Pico container.
Recommendation:	Approve-Conditional
Recommendation Constraints:	

Recommendation Justification:	XDoclet is still a viable code generation framework, but its use should be limited to situations when core Java annotations are not sufficient. XDoclet2 should not be introduced.

2.386) Xerces

General Information

Website:	http://xerces.apache.org/
Description:	Xerces is a project hosted by the Apache Software Foundation that consists of sub-projects that are focused on XML parser and related component development in the following languages; C++, Java, and Perl. There is also a sub-project, XML Commons, which is a set of XML components and utilities.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v3.2
Decision Date:	8/19/2009
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	ASF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JAXP Reference Implementation - ***(required for some configurations)***

Comparable Technologies/Standards:

- Castor XML

Companion Technologies/Standards:

- Xalan related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (07/07/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	The Xerces project represents a family of XML parsers that are individually released. For the latest release information on individual Xerces parsers, please refer to notes in the analysis summary section of this assessment.

General Analysis

Adoption Benefits

- Apache XML parsers are supported, widely used, and mature products.

Adoption Risks

- None significant.

Architectural Benefits

- None significant.

Architectural Risks

- None significant.

Standards Traceability

- XML 1.0, Fourth Edition
- XML 1.1, Second Edition
- Xinclude 1.0
- DOM Level 3
- XML Schema 1.0

General Assessment

Expected Usage:	Not defined.
Assessment Type:	New
Assessment Date:	7/7/2009
Notes:	Xerces XML parsers are individually released and updated. The current stable releases of Xerces parsers are: • Apache Xerces C++ 3.0.1 • Apache Xerces2 Java Parser 2.9.1 Xerces Perl has been tested on all operating systems listed in that

	section except HP-UX.
Recommendation:	Approve
Recommendation Constraints:	Apache Xerces Perl is excluded from the scope of this assessment.
Recommendation Justification:	The Xerces project represents a ten year effort to create and maintain XML parsers, APIs, and components offered in major programming languages. Xerces components are currently in use by multiple VA projects.

2.387) XML Namespaces (XML-NS)

General Information

Website:	http://www.w3.org/TR/xml-names11/
Description:	XML Namespaces (XML-NS) provide a simple method for qualifying element and attribute names used in eXtensible Markup Language (XML) documents by associating them with namespaces identified by Internationalized Resource Identifier (IRI) references.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRM Team
Vendor Name:	W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Extensible Markup Language (XML) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.1	8/16/2006		

VA Forecast Information (11/02/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

1.1	None	None	None	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Adoption Benefits

- Mature, widely adopted industry standard.

Architectural Benefits

- Reduction of XML markup vocabulary "collisions".
- Standardization/re-use of XML markup vocabularies.

General Assessment

Expected Usage:	Specification for XML element and attribute definitions.
Assessment Type:	Standard
Assessment Date:	11/2/2009
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	XML-NS provides a standard for XML markup vocabularies. Use of this standard will reduce the chances of namespace collisions.

2.388) XML Path Language (XPath)

General Information

Website:	http://www.w3.org/TR/
Description:	XML Path Language (Xpath) is an expression language that allows the processing of values conforming to the data model defined in Xquery/Xpath Data Model (XDM). The data model provides a tree representation of XML documents as well as atomic values such as integers, strings, and booleans, and sequences that may contain

both references to nodes in an XML document and atomic values. The result of an Xpath expression may be a selection of nodes from the input documents, or an atomic value, or more generally, any sequence allowed by the data model. The name of the language derives from its most distinctive feature, the path expression, which provides a means of hierarchic addressing of the nodes in an XML tree.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRM Team

Vendor Name: W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
XQuery/XPath Data Model (XDM)	This document defines the W3C XQuery and XPath Data Model (XDM), which is the data model of XPath, XSLT, and XQuery, and any other specifications that reference it.
XQuery/XPath Functions & Operations	This document defines constructor functions, operators and functions on the datatypes defined in XML Schema Part 2: Datatypes and the datatypes defined in XQuery 1.0 and XPath 2.0 Data Model. It also discusses functions and operators on nodes and node sequences as defined in the XQuery 1.0 and XPath 2.0 Data Model.
XQuery/XPath Formal Semantics	This document defines formally the semantics of XQuery 1.0 and XPath 2.0.
XQuery/XPath	This document defines constructor functions, operators and functions on

Full Text	the datatypes defined in XML Schema Part 2: Datatypes and the datatypes defined in XQuery 1.0 and XPath 2.0 Data Model. It also discusses functions and operators on nodes and node sequences as defined in the XQuery 1.0 and XPath 2.0 Data Model.
XML Path Language	XPath is an expression language that allows the processing of values conforming to the data model defined in [XQuery/XPath Data Model (XDM)]. The data model provides a tree representation of XML documents as well as atomic values such as integers, strings, and booleans, and sequences that may contain both references to nodes in an XML document and atomic values. The result of an XPath expression may be a selection of nodes from the input documents, or an atomic value, or more generally, any sequence allowed by the data model.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Extensible Markup Language (XML) - Standard
- XML Namespaces (XML-NS) - Standard
- XML Schema - Standard
- XQuery - Standard
- XSL Transformations (XSLT) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date

1.0	11/16/1999		
2.0	1/23/2007		

VA Forecast Information (11/02/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2.0	None	None	None	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Adoption Benefits

- XPath is a mature and widely adopted industry standard for querying XML documents.
- The XPath language is simple and concise.

Architectural Benefits

- Provides a single syntax for querying XML documents.

Architectural Risks

- None identified at this time.

General Assessment

Expected Usage: XML Query language for querying XML documents.

Assessment Type: New

Assessment Date: 11/2/2009

Notes:

Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	XPath is a mature, widely adopted industry standard for querying XML documents. XPath is concise, simple, and powerful.

2.389) XML Pointer Framework

General Information

Website:	http://www.w3.org/TR/xptr-framework/
Description:	The XML Pointer Language (XPointer) Framework is an extensible system for XML addressing that underlies additional XPointer scheme specifications.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Extensible Markup Language (XML) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	3/25/2003		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.0	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

Forecast Note:	

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.390) XML Schema

General Information

Website:	http://www.w3.org/XML/Schema
Description:	XML Schemas, also referred to as XML Schema Documents (XSDs), express shared vocabularies and allow machines to carry out rules made by people. They provide a means for defining the structure, content and semantics of XML documents in more detail.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRM Team
Vendor Name:	W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Namespaces	Recommended XML Namespace for Government Organizations

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Primer	Primer is a non-normative document intended to provide an easily readable description of the XML Schema facilities, and is oriented towards quickly understanding how to create schemas using the XML Schema language.
Structure	This document specifies the XML Schema definition language, which offers facilities for describing the structure and constraining the contents of XML 1.0 documents, including those which exploit the XML Namespace facility. The schema language, which is itself represented in XML 1.0 and uses namespaces, substantially reconstructs and considerably extends the capabilities found in XML 1.0 document type definitions (DTDs). This specification depends on XML Schema Part 2: Datatypes.
DataTypes	This document defines facilities for defining datatypes to be used in XML Schemas as well as other XML specifications. The datatype language, which is itself represented in XML 1.0, provides a superset of the capabilities found in XML 1.0 document type definitions (DTDs) for specifying datatypes on elements and attributes.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	898: Data Types / Validation

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Extensible Markup Language (XML) - Standard
- XML Namespaces (XML-NS) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	5/2/2001		
1.1	10/28/2004		

VA Forecast Information (11/02/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.1	None	None	None	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Adoption Benefits

- Mature, widely adopted industry standard

Adoption Risks

- Schemas can become verbose

Architectural Benefits

- XML content validation
- Strongly typed data structure definitions

General Assessment

Expected Usage:	Definition of structure, content, and semantics of XML based content.
Assessment Type:	Standard
Assessment Date:	11/2/2009
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	XML Schema is a mature, widely adopted industry standard that provides a specification for creating strongly type data structure definitions whose contents can be easily validated.

2.391) XML Signature Syntax and Processing (XML-Sig)

General Information

Website:	http://www.w3.org/TR/
Description:	XML Signature Syntax and Processing (XML-Sig) specifies XML digital signature processing rules and syntax. XML Signatures provide integrity, message authentication, and/or signer authentication services for data of any type, whether located within the XML that includes the signature or elsewhere.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	884: Certificates / Digital Signature

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Security Assertion Markup Language (SAML) - Standard
- Extensible Markup Language (XML) - Standard
- XML Namespaces (XML-NS) - Standard
- XML Path Language (XPath) - Standard
- XSL Transformations (XSLT) - Standard
- Multipurpose Internet Mail Extensions (MIME) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
IETF RFC 3275	3/1/2002		
1.0	2/12/2002		

2.0	6/10/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
IETF RFC 3275	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.392) XMLSpy

General Information

Website: http://www.altova.com/products/xmlspy/xml_editor.html

Description: XMLSpy is a markup language editor and integrated development environment for creating, modifying, transforming and debugging XML-related technologies. XMLSpy has a graphical schema designer, code generator, file converters, debuggers, profilers, relational database integration, and Visual Studio and Eclipse plug-ins. XMLSpy supports several standards and specifications such as XLST, Xpath, XQuery, WSDL, SOAP, XBRL, and OOXML.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source:	ARB
Decision Process:	TRM v3.1
Decision Date:	5/13/2009
Current Status:	Analysis Complete
Introduced By:	TRM Team
Vendor Name:	Altova

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	867: Integrated Development Environments (IDE)

Operating Systems Supported

- Red Hat Linux
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Eclipse - ***(required for some configurations)***
- XML Path Language (XPath) - ***(required libraries)***
- XSL Transformations (XSLT) - ***(required libraries)***
- XQuery - ***(required libraries)***
- XML Schema - ***(required libraries)***
- Extensible Markup Language (XML) - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2004	9/2/2003		
2004.3	10/28/2003		
2004.4	5/17/2004		
2005	10/3/2004		
2006	10/3/2005		
2006.3	6/1/2006		
2007	10/24/2006		
2007.3	5/30/2007		
2008	9/12/2007		
2008.2	4/29/2008		
2009	2/3/2009		

VA Forecast Information (10/27/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2004	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
2005	Supported	Supported	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated

2009	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment use of XML Spy is currently based on version 2005.

General Analysis

Architectural Area

- Application
- Integration
- Data

Architectural Benefits

- Common developer toolsets which support standardized skill sets, the implementation of best practices, as well as improvements in developer efficiency and effectiveness; all contribute to the architectural goals of reduced development risks and repeatable, consistent development practices for HeV.

EA Requirement

- ENTR909 - All applications and services shall reference the VHIM Template Registry (VTS) as the authoritative source/store for all VHIM implementation artifacts such as XML Schema Documents (XSD) and other metadata.
- ENTR1274 - Systems implementing VHA security audit shall be capable of converting standard audit to all of the following formats- XML, XLS, TXT, Comma Separated Value (CSV), DataBase File (DBF).
- ENTR1074 - VA OBJECTIVE E.3 Implement a One-VA information technology framework that enables the consolidation of IT solutions and the creation of cross-cutting common services to support the integration of information across business lines and provides secure, consistent, reliable, and accurate information to all interested parties.

Tool Type

- Tool

Tool Usage

- Development

General Assessment

Expected Usage: A commercial XML integrated development environment for development XML documents and specifications.

Assessment Type:	New
Assessment Date:	3/9/2009
Notes:	XMLSpy is a component of a larger bundle of development tools offered by Altova. Altova offers two suites of products, 2 different Mission Kits, which is targeted towards software architects and includes support for XML and web services development, data mapping and integration, publishing, UML modeling and database query and design. The 2nd Mission Kit is targeted at developers and doesn't include UML modeling or database query and design support.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	XMLSpy is a recognized industry leader for XML related development and support technologies.

2.393) XQuery

General Information

Website:	http://beta.w3.org/standards/techs/xquery
Description:	XQuery is a query and functional programming language that is designed to query collections of XML data. XQuery is an extension of XPath version 2.0. Any expression that is syntactically valid and executes successfully in both XPath 2.0 and XQuery will return the same result in both languages. Since these languages are so closely related, their grammars and language descriptions are generated from a common source to ensure consistency, and the editors of these specifications work closely together.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	Benefits Arch
Decision Process:	TRM v4.1

Decision Date: 10/28/2009
Current Status: Analysis Completed
Introduced By: Benefits ASA
Vendor Name: W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
XQuery/XPath Data Model (XDM)	This document defines the W3C XQuery and XPath Data Model (XDM), which is the data model of XPath, XSLT, and XQuery, and any other specifications that reference it.
XQuery/XPath Functions & Operations	This document defines constructor functions, operators and functions on the datatypes defined in XML Schema Part 2: Datatypes and the datatypes defined in XQuery 1.0 and XPath 2.0 Data Model. It also discusses functions and operators on nodes and node sequences as defined in the XQuery 1.0 and XPath 2.0 Data Model.
XQuery/XPath Formal Semantics	This document defines formally the semantics of XQuery and XPath.
XQuery/XPath Full Text	This document defines constructor functions, operators and functions on the datatypes defined in XML Schema Part 2: Datatypes and the datatypes defined in XQuery 1.0 and XPath 2.0 Data Model. It also discusses functions and operators on nodes and node sequences as defined in the XQuery 1.0 and XPath 2.0 Data Model.
XQuery 1.0: An XML Query Language	XML is a versatile markup language, capable of labeling the information content of diverse data sources including structured and semi-structured documents, relational databases, and object repositories. A query language that uses the structure of XML intelligently can express queries across all these kinds of data, whether physically stored in XML or viewed as XML via middleware. This specification describes a query language called XQuery, which is designed to be broadly applicable across many types of XML data sources.

FEA Categories

Service Area	Service Category	Service Standard Code

Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Structured Query Language (SQL)
- XSL Transformations (XSLT)

Companion Technologies/Standards:

- Extensible Markup Language (XML) - Standard
- XML Namespaces (XML-NS) - Standard
- XML Schema - Standard
- XML Path Language (XPath) - Standard
- XLink - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	1/23/2007		

VA Forecast Information (10/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009	CY2010	CY2011

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.0	None	None	None	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Adoption Benefits

- XQuery is a widely adopted industry standard
- XQuery is easier to learn than XSLT

Adoption Risks

- XQuery is limited to static analysis as it lacks dynamic binding

Architectural Benefits

- Data Integration - provides select, filter, transform, join, and aggregate data capabilities across multiple data sources
- Expressiveness - XQuery can query many different data structures and its recursive nature makes it ideal for querying tree and graph structures
- Brevity - XQuery statements are shorter than similar SQL or XSLT programs
- Flexibility - XQuery can query both hierarchical and tabular data
- Consistency - XQuery has a consistent syntax and can be used with other XML standards such as XML Schema datatypes

General Assessment

Expected Usage:	To extract and manipulate data from XML documents or any data source that can be viewed as XML.
Assessment Type:	Standard
Assessment Date:	11/2/2009
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	XQuery is a widely adopted industry standard for finding, extracting and manipulating data from XML documents. It provides a powerful database query capability similar to that of SQL.

2.394) XSL Transformations (XSLT)

General Information

Website:	http://www.w3.org/TR/xslt20
Description:	The XSL Transformations (XSLT) specification defines the syntax and semantics of XSLT 2.0, a language for transforming XML documents into other XML documents. XSLT 2.0 is designed to be used in conjunction with XPath 2.0. XSLT shares the same data model as XPath 2.0 and it uses the library of functions and operators defined in Xpath. XSLT 2.0 also includes optional facilities to serialize the results of a transformation, by means of an interface to the serialization component.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	Benefits Arch
Decision Process:	TRM v4.1
Decision Date:	10/28/2009
Current Status:	Analysis Completed
Introduced By:	Benefits ASA
Vendor Name:	W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	899: Data Transformation

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- XQuery

Companion Technologies/Standards:

- Extensible Markup Language (XML) - Standard
- XML-Infoset - Standard
- XML Namespaces (XML-NS) - Standard
- XML Schema - Standard
- XML Path Language (XPath) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	11/16/1999		
2.0	1/23/2007		

VA Forecast Information (10/05/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2.0	None	None	None	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Adoption Benefits

- XSLT is a mature and widely adopted industry standard for transforming XML documents.

Adoption Risks

- Declarative languages such as XSLT may incur a performance penalty and require greater resources.

Architectural Benefits

- XSLT applications for transforming XML data structures can be made much more resilient to changes in the details of the XML documents than a procedural application coded using the low-level DOM and SAX interfaces. This leads to data independence.
- Supports multiple output processing from a single XSLT transformation, enabling the production of multiple instances of XML, HTML, xHTML, or text outputs. This increases interoperability.
- Supports multiple input processing, including non-XML formats such as HTML, xHTML, and delimited files. This increases interoperability.

General Assessment

Expected Usage:	Support XML document transformation requirements.
Assessment Type:	New
Assessment Date:	11/18/2009
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendati	XSLT is a mature, widely adopted industry standard. It provides a

on Justification: specification for transforming XML documents.

2.395) z/OS

General Information

Website: http://www-03.ibm.com/systems/z/os/zos/

Description: z/OS is a 64-bit graphical user interface based operating system for mainframe computers. It is the successor to OS/390, which in turn followed MVS and combined a number of formerly separate, related products.

Decision: Approved

Decision Constraints: Products that have been deployed to a production environment may continue to use this technology. All other products must utilize a One-VA TRM approved Linux operating system.

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: CDCO Supported Architecture Components

Vendor Name: IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	866: Dependent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.5	3/26/2004		3/31/2007
1.6	9/24/2004		9/30/2007
1.7	9/30/2005		9/30/2008
1.8	9/29/2006		9/30/2009
1.9	9/28/2007		9/30/2010
1.10	9/26/2008		
1.11	9/25/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009	CY2010	CY2011

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.5	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.6	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.7	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.8	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.9	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.10	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

2.396) z/VM

General Information

Website: http://www.vm.ibm.com/

Description: z/VM is a 64-bit virtual machine operating system. It can be used to support large numbers (thousands) of Linux virtual machines.

Decision: Approved

Decision Constraints: Products that have been deployed to a production environment may continue to use this technology. All other products must utilize a One-VA TRM approved Linux operating system.

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: CDCO Supported Architecture Components

Vendor Name: IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	866: Dependent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5.3	6/29/2007		
5.4	9/12/2008		
6.1	10/23/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
5.3	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

3) Approved Benefits Segment Technologies/Standards List

Name	Vendor	Deciding Source	Decision Process	Decision Date
7 kHz Audio-Coding within 64 kbit/s *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
A Framework for IP Based Virtual Private Networks (VPNs) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Access Control		EA	TRMSP 4.3.2	3/14/2008
Access Control Framework *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
Active Data Guard *(2)(3)*	Oracle	CDCO	CDCO 6.15.2009	6/15/2009
Advanced Encryption Standard (AES) *(1)*	NIST	EA	TRMSP 4.3.2	3/14/2008
Advanced Video Coding for Generic Audiovisual Services *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
ANT *(2)*	ASF	ARB	TRM v2	9/17/2008
Apache Commons *(2)*	ASF	ARB	TRM v3	1/7/2009
Apache Struts *(2)(3)*	ASF	ARB	TRM v2	9/17/2008
Apache Tomcat *(2)(3)*	ASF	CDCO	CDCO 6.15.2009	6/15/2009

Application Oriented Sites		EA	TRMSP 4.3.2	3/14/2008
Architecture for IP Address Allocation with CIDR *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Audit Services		EA	TRMSP 4.3.2	3/14/2008
Basic Transition Mechanisms for IPv6 Hosts Routers *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Biometric Application Programming Interface (BioAPI) *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
Biometric Information Management and Security *(1)*	ANSI	EA	TRMSP 4.3.2	3/14/2008
Biometric Services		EA	TRMSP 4.3.2	3/14/2008
BMC Mainview *(2)(3)*	BMC Software	CDCO	CDCO 6.15.2009	6/15/2009
Border Gateway Protocol (BGP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Broadband Audiovisual Communication Systems and Terminals *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Call Signalling Protocols and Media Stream Packetization *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Carrier Sense Multiple Access with Collision Detection (CSMA/CD) *(1)*	IEEE	EA	TRMSP 4.3.2	3/14/2008
Cascading Style Sheets (CSS) *(1)*	W3C	EA	TRMSP 4.3.2	3/14/2008
Cascading Style Sheets Mobile Profile (CSS-Mobile) *(1)*	W3C	EA	TRMSP 4.3.2	3/14/2008
Checksum Hash Value		EA	TRMSP 4.3.2	3/14/2008
Classless Inter-Domain Routing (CIDR) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Coding of Speech Using Low-Delay Code Excited Linear Prediction *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Common Biometric Exchange Formats Framework (CBEFF) *(1)*	NIST	EA	TRMSP 4.3.2	3/14/2008
Common Language Infrastructure (CLI) *(1)*	ECMA	EA	TRMSP 4.3.2	3/14/2008
Common Object Request Broker Architecture (CORBA) *(1)*	OASIS	EA	TRMSP 4.3.2	3/14/2008
Common Warehouse Metamodel (CWM) *(1)*	OMG	EA	TRMSP 4.3.2	3/14/2008
Computer Based Training Exchange		EA	TRMSP 4.3.2	3/14/2008
Computer Graphics Metafile (CGM) *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
Confidentiality Framework *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
Confidentiality Services		EA	TRMSP 4.3.2	3/14/2008
Configuration Management		EA	TRMSP 4.3.2	3/14/2008
Control Protocol for Multimedia Communication *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Cryptographic Algorithm Implementation Requirements for ESP and AH *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Data Center *(1)*		EIE CTO	TAR-TAS	11/13/2009
Data Encryption Standard (DES) *(1)*	NIST	EA	TRMSP 4.3.2	3/14/2008
Data Format Classification		EA	TRMSP 4.3.2	3/14/2008
Data Format for Fingerprint, Facial, & SMT Information *(1)*	NIST	EA	TRMSP 4.3.2	3/14/2008

Data Integrity		EA	TRMSP 4.3.2	3/14/2008
Data Oriented Sites		EA	TRMSP 4.3.2	3/14/2008
Data Protocols for Multimedia Conferencing *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Data Protocols for Multimedia Conferencing - Generic Conference Control *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Database Services		EA	TRMSP 4.3.2	3/14/2008
Datatypes for DTDs (DT4DTD) *(1)*	W3C	EA	TRMSP 4.3.2	3/14/2008
Differentiated Services (DS) Field in IPv4 and IPv6 Headers *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Digital Compression and Coding of Continuous-Tone Still Images *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
Digital Signature		EA	TRMSP 4.3.2	3/14/2008
Digital Signature Standard (DSS) *(1)*	NIST	EA	TRMSP 4.3.2	3/14/2008
Dimensions CM *(2)(3)*	Serena Software	Benefits Arch	TRM v4.1	10/28/2009
Directory Server *(2)(3)*	Oracle	CDCO	CDCO 6.15.2009	6/15/2009
Discovery Services		EA	TRMSP 4.3.2	3/14/2008
Diskeeper *(2)(3)*	Diskeeper Corp.	CDCO	CDCO 6.15.2009	6/15/2009
Domain Name Service		EA	TRMSP 4.3.2	3/14/2008
Domain Name System (DNS) Configuration Options *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Domain Name System (DNS) Extensions *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Domain Name System (DNS) Structure and Delegation *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Dynamic Host Configuration Protocol (DHCP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Dynamic Host Configuration Protocol Configuration of IPsec Tunnel Mode (DHCPv4) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Dynamic Host Configuration Protocol for IPv6 (DHCPv6) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Dynamic Server Side Display		EA	TRMSP 4.3.2	3/14/2008
Dynamic Updates in the Domain Name System (DNS UPDATE) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
ebXML Collaboration Protocol Profile and Agreement (ebXML CPPA) *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
ebXML Messaging Service (ebMS) *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
ebXML Registry Information Model (ebRIM) *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
ebXML Registry Services (ebRS) *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
Eclipse *(2)*	Eclipse	ARB	TRM v2	9/17/2008
Eclipse WTP *(2)*	Eclipse	Benefits Arch	TRM v4.1	10/28/2009
eGate Integrator *(2)(3)*	Oracle	CDCO	CDCO 6.15.2009	6/15/2009
Encryption Algorithm and IPsec *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008

Encryption Services		EA	TRMSP 4.3.2	3/14/2008
Enhanced Security Services for S/MIME *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Escrowed Encryption Standard *(1)*	NIST	EA	TRMSP 4.3.2	3/14/2008
Establishing Communication Between Multiple Audiovisual Terminals *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
European Article Number (EAN-13) *(1)*	GS1	EA	TRMSP 4.3.2	3/14/2008
Exchange Server *(2)(3)*	Microsoft	CDCO	CDCO 6.15.2009	6/15/2009
Extended Simple Mail Transfer Protocol (ESMTP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
eXtensible Access Control Markup Language (XACML) *(1)*	OASIS	EA	TRMSP 4.3.2	3/14/2008
Extensible Authentication Protocol (EAP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Extensible Authentication Protocol Tunneled Transport Layer Security (EAP-TTLS) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Extensible HyperText Markup Language (XHTML) *(1)*	W3C	EA	TRMSP 4.3.2	3/14/2008
Extensible Markup Language (XML) *(1)*	W3C	Benefits Arch	TRM v4.1	10/28/2009
Fault Management		EA	TRMSP 4.3.2	3/14/2008
FDR *(2)(3)*	Innovation	CDCO	CDCO 6.15.2009	6/15/2009
Fiber Distributed Data Interface (FDDI) *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
File Transfer Protocol (FTP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
File Transfer Protocol (FTP) Extensions *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
File Transfer Protocol Services		EA	TRMSP 4.3.2	3/14/2008
FileNet P8 *(2)*	IBM	Benefits Arch	TRM v4.1	10/28/2009
Fire Walling		EA	TRMSP 4.3.2	3/14/2008
Firefox *(2)*	Mozilla	ARB	TRM v2	9/17/2008
Frame Structure in Audiovisual Teleservices *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Frame-synchronous Control and Indication Signals for Audiovisual Systems *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
General Parallel File System (GPFS) *(2)(3)*	IBM	CDCO	CDCO 6.15.2009	6/15/2009
Graphics Interchange Format (GIF) *(1)*	W3C	EA	TRMSP 4.3.2	3/14/2008
Health Information Data Exchange		EA	TRMSP 4.3.2	3/14/2008
HyperText Markup Language (HTML) *(1)*	W3C	EA	TRMSP 4.3.2	3/14/2008
Hypertext Transfer Protocol (HTTP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Hypertext Transfer Protocol Services		EA	TRMSP 4.3.2	3/14/2008
Identification Authentication		EA	TRMSP 4.3.2	3/14/2008
Identification Cards - Integrated Circuit(s) Cards With Contacts *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
Internet Control Message Protocol (ICMP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Internet Explorer *(2)*	Microsoft	ARB	TRM v2	9/17/2008
Internet Key Exchange (IKE) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008

Internet Message Access Protocol (IMAP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Internet Message Format *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Internet Protocol (IP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Internet Protocol Version 6 (IPv6) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Internet Web		EA	TRMSP 4.3.2	3/14/2008
Intranet Web		EA	TRMSP 4.3.2	3/14/2008
Intrusion Detection and Prevention Systems (IDPS) *(1)*	NIST	EA	TRMSP 4.3.2	3/14/2008
Intrusion Detection Devices		EA	TRMSP 4.3.2	3/14/2008
IP Authentication Header (AH) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
IP Encapsulating Security Payload (ESP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
IP Network Address Translator (NAT) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
IP Routing Services*(3)*		EA	TRMSP 4.3.2	3/14/2008
IPsec Transport Mode for Dynamic Routing *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
IPsec-Network Address Translation (NAT) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
IPv6 Client Services		EA	TRMSP 4.3.2	3/14/2008
IPv6 over Point-to-Point Protocol (PPP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
IPv6 Performance		EA	TRMSP 4.3.2	3/14/2008
IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCPv6) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
IPv6/IPv4 Dual Stack Internet Access Service Model *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Java Data Objects (JDO) *(1)*	Sun Microsystems	EA	TRMSP 4.3.2	3/14/2008
Java EE *(1)*	Sun Microsystems	ARB	TRM v2	9/17/2008
Java SE *(1)*	Sun Microsystems	ARB	TRM v2	9/17/2008
JAXB Reference Implementation *(2)*	Sun Microsystems	ARB	TRM v2	9/17/2008
JAXP Reference Implementation *(2)*	Sun Microsystems	ARB	TRM v2	9/17/2008
JPEG *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
JPEG 2000 *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
JRules Business Rules Management Server *(2)*	ILOG	ARB	TRM v3.1	5/13/2009
JRules Rule Execution Server *(2)*	ILOG	ARB	TRM v3.1	5/13/2009
JRules Rule Studio *(2)*	ILOG	ARB	TRM v3.1	5/13/2009
JRules Scenario Manager *(2)*	ILOG	ARB	TRM v3.1	5/13/2009
JRules Team Server *(2)*	ILOG	ARB	TRM v3.1	5/13/2009
JUnit *(2)*	SourceForge	ARB	TRM v2	9/17/2008
Key Management Using ANSI X9.17 *(1)*	NIST	EA	TRMSP 4.3.2	3/14/2008

Keyed-Hash Message Authentication Code (HMAC) *(1)*	NIST	EA	TRMSP 4.3.2	3/14/2008
Layer Two Tunneling Protocol (L2TP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Lightweight EAP (LEAP) *(1)*		EA	TRMSP 4.3.2	3/14/2008
LiveCycle *(2)(3)*	Adobe	Benefits Arch	TRM v4.1	10/28/2009
Local Area Network (LAN) *(1)*		EIE CTO	TAR-TAS	11/5/2009
Log4J *(2)*	ASF	ARB	TRM v2	9/17/2008
Mail Services		EA	TRMSP 4.3.2	3/14/2008
Malicious Code Detection		EA	TRMSP 4.3.2	3/14/2008
Management Information Base (MIB) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Media Servers		EA	TRMSP 4.3.2	3/14/2008
Medical Device Interoperability		EA	TRMSP 4.3.2	3/14/2008
Medical Radiology Images Exchange		EA	TRMSP 4.3.2	3/14/2008
Metropolitan Area Network Services		EA	TRMSP 4.3.2	3/14/2008
Mirth Connect *(2)(3)*	Mirth Corp.	CDCO	CDCO 6.15.2009	6/15/2009
MPEG-1 *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
MPEG-2 *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
MPEG-4 *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
Multimedia Transport*(3)*		EA	TRMSP 4.3.2	3/14/2008
Multiplexing Protocol for Low Bit Rate Multimedia Communication *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Multipoint Binary File Transfer Protocol *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Multipoint Communication Service (MCS) - Service Definition *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Multipoint Communication Service (MCS) Protocol *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Multipoint Control Units for Audiovisual Systems *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Multipoint Still Image and Annotation Protocol *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Multiprotocol Label Switching (MPLS) Architecture *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Multipurpose Internet Mail Extensions (MIME) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Narrow-band Visual Telephone Systems and Terminal Equipment *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Native Audio Formats		EA	TRMSP 4.3.2	3/14/2008
Native Document Formats		EA	TRMSP 4.3.2	3/14/2008
Native Graphics Formats		EA	TRMSP 4.3.2	3/14/2008
Native Video Formats		EA	TRMSP 4.3.2	3/14/2008
Neighbor Discovery for IPv6 *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
NetBackup *(2)(3)*	Symantec	CDCO	CDCO 6.15.2009	6/15/2009
Network Address Translation - Protocol Translation (NAT-PT) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Network Transport		EA	TRMSP 4.3.2	3/14/2008

Network-specific Data Protocol Stacks for Multimedia Conferencing *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Object Linking and Embedding, Database (OLE DB) *(1)*	Microsoft	EA	TRMSP 4.3.2	3/14/2008
Objects and Attributes for Access Control *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
Office Open XML *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
Open Database Connectivity (ODBC) *(1)*	Microsoft	EA	TRMSP 4.3.2	3/14/2008
Open Graphics Library (OpenGL) *(1)*	OpenGL	EA	TRMSP 4.3.2	3/14/2008
Open Shortest Path First (OSPF) Protocol *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
OpenVMS *(2)(3)*	HP	CDCO	CDCO 6.15.2009	6/15/2009
Oracle Database *(2)(3)*	Oracle	ARB	TRM v2	9/17/2008
Oracle RAC *(2)(3)*	Oracle	Benefits Arch	TRM v4.1	10/28/2009
Packet-Based Multimedia Communications Systems *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Parallel Sysplex *(2)(3)*	IBM	CDCO	CDCO 6.15.2009	6/15/2009
Password Services		EA	TRMSP 4.3.2	3/14/2008
Performance Management		EA	TRMSP 4.3.2	3/14/2008
Pharmacological Orders Exchange		EA	TRMSP 4.3.2	3/14/2008
PlateSpin Migrate *(2)(3)*	Novell	CDCO	CDCO 6.15.2009	6/15/2009
PlateSpin PowerConvert *(2)(3)*	Novell	CDCO	CDCO 6.15.2009	6/15/2009
PlateSpin Protect *(2)(3)*	Novell	CDCO	CDCO 6.15.2009	6/15/2009
Point-to-Point Protocol (PPP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Portable Document Format (PDF) *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
Portable Network Graphics (PNG) *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
Portlet *(1)*	Sun Microsystems	EA	TRMSP 4.3.2	3/14/2008
Post Office Protocol (POP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
PPP Triple-DES Encryption Protocol (3DESE) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Processor Area Network (PAN) Manager *(2)(3)*	Egenera	CDCO	CDCO 6.15.2009	6/15/2009
Protected Extensible Authentication Protocol (PEAP) *(1)*	Microsoft	EA	TRMSP 4.3.2	3/14/2008
Public Key Infrastructure		EA	TRMSP 4.3.2	3/14/2008
Pulse Code Modulation (PCM) of Voice Frequencies *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Radio Frequency Management		EA	TRMSP 4.3.2	3/14/2008
Rational ClearCase with MultiSite *(2)(3)*	IBM	ARB	TRM v2	9/17/2008
Rational Software Modeler *(2)(3)*	IBM	ARB	TRM v2	9/17/2008
Regulations and Procedures for Federal Radio Frequency Management *(1)*	NTIA	EA	TRMSP 4.3.2	3/14/2008
Remote Access Protocol		EA	TRMSP 4.3.2	3/14/2008
Remote Authentication Dial In User Service (RADIUS) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Rich Text Format (RTF) *(1)*	Microsoft	EA	TRMSP 4.3.2	3/14/2008
Scalable Vector Graphics (SVG) *(1)*	W3C	EA	TRMSP 4.3.2	3/14/2008

Secure Code Design		EA	TRMSP 4.3.2	3/14/2008
Secure Hash Standard (SHS) *(1)*	NIST	EA	TRMSP 4.3.2	3/14/2008
Secure Hypertext Transfer Protocol (S-HTTP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Secure Remote Access with L2TP *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Secure/Multipurpose Internet Mail Extensions (S/MIME) Certificate Handling *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Secure/Multipurpose Internet Mail Extensions (S/MIME) Message Spec *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Securing Layer Two Tunneling Protocol (L2TP) with IPsec *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Security Architecture for the Internet Protocol (IP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Security Architecture for the Internet Protocol (IPSec) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Security Assertion Markup Language (SAML) *(1)*	OASIS	Benefits Arch	TRM v4.1	10/28/2009
Security Requirements for Cryptographic Modules *(1)*	NIST	EA	TRMSP 4.3.2	3/14/2008
Security Token		EA	TRMSP 4.3.2	3/14/2008
Servers *(1)*		EIE CTO	TAR-TAS	11/18/2009
SharePoint Server *(2)(3)*	Microsoft	CDCO	CDCO 6.15.2009	6/15/2009
Simple Mail Transfer Protocol (SMTP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Simple Network Management Protocol (SNMP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Simple Object Access Protocol (SOAP) *(1)*	W3C	Benefits Arch	TRM v4.1	10/28/2009
Single Sign On		EA	TRMSP 4.3.2	3/14/2008
Solaris *(2)(3)*	Sun Microsystems	ARB	TRM v2	9/17/2008
Stateless Dynamic Host Configuration Protocol (DHCPv6) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Static Display		EA	TRMSP 4.3.2	3/14/2008
Storage *(1)*		EIE CTO	TAR-TAS	11/18/2009
Strobe *(1)(3)*	Compuware	CDCO	CDCO 6.15.2009	6/15/2009
Structured Query Language (SQL) *(1)*	ANSI	Benefits Arch	TRM v4.1	10/28/2009
Synchronous Optical Network (SONET) *(1)*	ANSI	EA	TRMSP 4.3.2	3/14/2008
System for Establishing Communication Between Audiovisual Terminals *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
TELNET *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Temporal Key Integrity Protocol (TKIP) *(1)*	IEEE	EA	TRMSP 4.3.2	3/14/2008
Teredo *(1)(3)*	Microsoft	CDCO	CDCO 6.15.2009	6/15/2009
Transmission of IP Datagrams over SMDS *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Transport Layer Security (TLS) Protocol *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
TreeSize *(2)(3)*	JAM Software	CDCO	CDCO 6.15.2009	6/15/2009
Triple Data Encryption Algorithm (TDEA) Block Cipher *(1)*	NIST	EA	TRMSP 4.3.2	3/14/2008

Uniform Resource Identifiers (URI) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
Universal Description, Discovery, and Integration (UDDI) *(1)*	OASIS	Benefits Arch	TRM v4.1	10/28/2009
Universal Healthcare Identifier (UHID) *(1)*	ASTM	EA	TRMSP 4.3.2	3/14/2008
UNIX *(1)*	The Open Group	EA	TRMSP 4.3.2	3/14/2008
Unsolicited Email		EA	TRMSP 4.3.2	3/14/2008
User Datagram Protocol (UDP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
vConverter *(2)(3)*	Quest Software	CDCO	CDCO 6.15.2009	6/15/2009
Veritas Storage Foundation *(2)(3)*	Symantec	CDCO	CDCO 6.15.2009	6/15/2009
Video Codec for Audiovisual Services *(1)*	ITU	EA	TRMSP 4.3.2	3/14/2008
Virtual Bridged Local Area Networks (VLAN) *(1)*	IEEE	EA	TRMSP 4.3.2	3/14/2008
VLAN Trunking Protocol (VTP) *(1)*	Cisco	EA	TRMSP 4.3.2	3/14/2008
VM Performance Toolkit *(2)(3)*	IBM	CDCO	CDCO 6.15.2009	6/15/2009
VMware Site Recovery Manager *(2)(3)*	VMware	CDCO	CDCO 6.15.2009	6/15/2009
VMware vCenter CapcityIQ *(2)(3)*	VMware	CDCO	CDCO 6.15.2009	6/15/2009
VMware vCenter Chargeback *(2)(3)*	VMware	CDCO	CDCO 6.15.2009	6/15/2009
VMware vCenter Lab Manager *(2)(3)*	VMware	CDCO	CDCO 6.15.2009	6/15/2009
VMware vCenter Server Heartbeat *(2)(3)*	VMware	CDCO	CDCO 6.15.2009	6/15/2009
VMware vSphere *(2)(3)*	VMware	CDCO	CDCO 6.15.2009	6/15/2009
VPN Services		EA	TRMSP 4.3.2	3/14/2008
vRanger Pro *(2)(3)*	Quest Software	CDCO	CDCO 6.15.2009	6/15/2009
Warehouse Services		EA	TRMSP 4.3.2	3/14/2008
Web Services Description Language (WSDL) *(1)*	W3C	ARB	TRM v2	9/17/2008
WebLogic Server *(2)*	Oracle	ARB	TRM v2	9/17/2008
Wide Area Network (WAN) *(1)*		EIE CTO	TAR-TAS	11/30/2009
Wi-Fi Protected Access (WPA) *(1)*	Wi-Fi Alliance	EA	TRMSP 4.3.2	3/14/2008
Wily Introscope *(2)(3)*	CA	CDCO	CDCO 6.15.2009	6/15/2009
Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) *(1)*	IEEE	EA	TRMSP 4.3.2	3/14/2008
Wireless Mobile Voice		EA	TRMSP 4.3.2	3/14/2008
Wireless Transport Layer Security (WTLS) *(1)*	OMA	EA	TRMSP 4.3.2	3/14/2008
WS-Reliable Messaging *(1)*	OASIS	Benefits Arch	TRM v4.1	10/28/2009
WS-Security *(1)*	OASIS	Benefits Arch	TRM v4.1	10/28/2009
X.500 The Directory *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
X.509 Certificate Request Message Format (CRMF) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
X.509 PKI Representation of Key Exchange Algorithm (KEA) Keys *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
X.509 Public Key Infrastructure (PKI) Certificate and CRL	IETF	EA	TRMSP 4.3.2	3/14/2008

Profile *(1)*				
X.509 Public Key Infrastructure (PKI) Certificate Management Protocols *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
X.509 Public Key Infrastructure LDAP Schema *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
X.509 Public Key Infrastructure Online Certificate Status Protocol (OCSP) *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
X.509 Public Key Infrastructure Operational Protocols: LDAP *(1)*	IETF	EA	TRMSP 4.3.2	3/14/2008
X.509 Public-Key and Attribute Certificate Frameworks *(1)*	ISO	EA	TRMSP 4.3.2	3/14/2008
XML Namespaces (XML-NS) *(1)*	W3C	EA	TRMSP 4.3.2	3/14/2008
XML Path Language (XPath) *(1)*	W3C	EA	TRMSP 4.3.2	3/14/2008
XML Pointer Framework *(1)*	W3C	EA	TRMSP 4.3.2	3/14/2008
XML Schema *(1)*	W3C	EA	TRMSP 4.3.2	3/14/2008
XML Signature Syntax and Processing (XML-Sig) *(1)*	W3C	EA	TRMSP 4.3.2	3/14/2008
XMLSpy *(2)*	Altova	ARB	TRM v3.1	5/13/2009
XQuery *(1)*	W3C	Benefits Arch	TRM v4.1	10/28/2009
XSL Transformations (XSLT) *(1)*	W3C	Benefits Arch	TRM v4.1	10/28/2009
z/OS *(2)(3)*	IBM	CDCO	CDCO 6.15.2009	6/15/2009
z/VM *(2)(3)*	IBM	CDCO	CDCO 6.15.2009	6/15/2009

(1) - Indicates a standard or specification. It is in no way an endorsement or approval for technologies that implement the standard or specification.

(2) - Indicates a technology.

(3) - Indicates a constraint.

4) Approved Benefits Segment Technologies/Standards Entries

4.1) 7 kHz Audio-Coding within 64 kbit/s

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=G

Description: ITU-T G.722: 7 kHz Audio-Coding within 64 kbit/s describes the characteristics of an audio (50 to 7,000 Hz) coding system which may be used for a variety of higher quality speech applications. The coding system uses sub-band adaptive differential pulse code

modulation (SB-ADPCM) within a bit rate of 64 kbit/s.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.3	11/24/2006		
1.4	11/24/2006		
1.5	7/6/2007		
1.6	11/6/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.4	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.2) A Framework for IP Based Virtual Private Networks (VPNs)

General Information

Website: http://tools.ietf.org/html/rfc2764

Description: A Framework for IP Based Virtual Private Networks (VPNs) describes a framework for VPNs running across IP backbones. It discusses the various different types of VPNs, their respective requirements, and proposes specific mechanisms that could be used to implement each type of VPN using existing or proposed specifications. The objective of this document is to serve as a framework for related protocol development in order to develop the full set of specifications required for widespread deployment of interoperable VPN solutions.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2764	2/1/2000		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2764	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.3) Access Control

General Information

Description: Access control services prevent the unauthorized use of information system resources. These services may be applied to various aspects of access to a resource (e.g., access to communications with the resource; the reading, writing; or deletion of an information or data resource; or the execution of a processing resource) or to all accesses to a resource.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Scope		Access Controls will be applied according to VA Handbook 6500: Cyber Security and IETF RFC 2196: Site Security Handbook for services like TELNET, CGI, and FTP, which may access VA protected servers.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description

Access Services	Authorized system administrators should be the only ones allowed to perform access services like telnet and rlogin.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.4) Access Control Framework

General Information

Website:	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18199
Description:	ISO/IEC 10181-3: Access Control Framework specifies a general framework for the provision of access control. The purpose of access control is to counter the threat of unauthorized operations involving a computer or communication system.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2

Decision Date: 3/14/2008
Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date

1996	1/1/1996		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1996	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.5) Active Data Guard

General Information

Website: http://www.oracle.com/technology/deploy/availability/htdocs/DataGuardOverview.html

Description: Active Data Guard provides the management, monitoring, and automation software to create and maintain one or more synchronized replicas (standby databases) of a production database (primary database). An Active Data Guard standby database is an exact copy of the primary that is open read-only while it continuously applies changes transmitted by the primary database.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	Oracle

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Database/Storage	875: Database

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- Oracle Database - ***(required libraries)***
- Oracle RAC - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Transmission Control Protocol (TCP) related as: (Companion)
- Internet Protocol (IP) related as: (Companion)
- Structured Query Language (SQL) related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	See Oracle Database for Release and VA Forecast information.

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.6) Advanced Encryption Standard (AES)

General Information

Website: http://csrc.nist.gov/publications/PubsFIPS.html

Description: FIPS 197: Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext;

	decrypting the ciphertext converts the data back into its original form, called plaintext.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	NIST

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1	11/1/2001		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.7) Advanced Video Coding for Generic Audiovisual Services

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=H

Description: Advanced Video Coding for Generic Audiovisual Services is

designed to enable the use of the coded video representation in a flexible manner for a wide variety of network environments. The use of this coding standard allows motion video to be manipulated as a form of computer data and to be stored on various storage media, transmitted and received over existing and future networks and distributed on existing and future broadcasting channels.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1	5/30/2003		
2	3/1/2005		
3	11/22/2007		
4	3/16/2009		
5	3/9/2010		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.8) ANT

General Information

Website: http://ant.apache.org

Description: ANother build Tool (ANT) is a Java-based build tool. ANT is similar to Make, but has greater cross platform compatibility. Make is extended with shell-based commands limited to the operating system; ANT is extended using Java classes-eliminating the need to write shell commands. ANT also uses XML-based configuration files that call out a target tree for executing various tasks in the Java compilation and build process.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: ARB

Decision Process: TRM v2

Decision Date: 9/17/2008

Current Status: Analysis Completed

Introduced By: Extended Tool List (ETL)

Vendor Name: ASF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	868: Software Configuration Management

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required for some configurations)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.6.0	12/18/2003		
1.6.1	2/14/2004		
1.6.2	7/16/2004		
1.6.3	4/28/2005		
1.6.4	5/19/2005		
1.6.5	6/2/2005		
1.7.0	12/19/2006		
1.7.1	6/27/2008		

VA Forecast Information (10/14/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the

responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.7.0	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.7.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment development and deployment of ANT is currently based on version 1.6.5.

General Analysis

Architectural Area

- Integration

Standards Traceability

- SGML (ISO 8879)

Tool Type

- Framework

Tool Usage

- Development

General Assessment

Expected Usage:	ANT provides a framework for scripting software builds, installation and configuration tasks.
Assessment Type:	Refresh
Assessment Date:	9/15/2008
Notes:	ANT is the leading framework automating build, configuration, installation and test execution. Although Maven is an alternative to ANT, they have different architectures; most projects will not be

	able to move from ANT to Maven without a major restructuring of the source code directory structure.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	ANT has been successfully implemented in the HeV infrastructure.

4.9) Apache Commons

General Information

Website:	http://commons.apache.org/
Description:	Formerly listed on the TRM as "Jakarta Commons Collections". Apache Commons is an open source project focused on all aspects of creating and maintaining a library of reusable Java components. One of the primary goals of the Apache Commons project is to ensure that the components have minimal dependencies on other libraries, to make deployments easier. Similarly, Commons components will keep their interfaces as stable as possible, so that end-users (including HeV projects) can implement these components without having to worry about future changes breaking deployed source code.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v3
Decision Date:	1/7/2009
Current Status:	Analysis Completed
Introduced By:	TRM Team
Vendor Name:	ASF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Attributes	Runtime API to metadata attributes such as doclet tags.
BeanUtils	Easy-to-use wrappers around the Java reflection and introspection APIs
Betwixt	Services for mapping JavaBeans to XML documents, and vice versa
Chain	"Chain of Responsibility" pattern implementation
CLI	Command Line arguments parser
Codec	General encoding/decoding algorithms (for example phonetic, base64, URL)
Collections	Extends or augments the Java Collections Framework
Configuration	Reading of configuration/preferences files in various formats
Daemon	Alternative invocation mechanism for unix-daemon-like java code
DBCP	Database connection pooling services
DbUtils	JDBC helper library
Digester	XML-to-Java-object mapping utility
Discovery	Tools for locating resources by mapping service/reference names to resource names
EL	Interpreter for the Expression Language defined by the JSP 2.0 specification
Email	Library for sending e-mail from Java
Exec	API for dealing with external process execution and environment management in Java
FileUpload	File upload capability for your servlets and web applications
IO	Collection of I/O utilities
JCI	Java Compiler Interface
Jelly	XML based scripting and processing engine
Jexl	Expression language which extends the Expression Language of the JSTL
JXPath	Utilities for manipulating Java Beans using the XPath syntax
Lang	Provides extra functionality for classes in java.lang
Launcher	Cross platform Java application launcher
Logging	Wrapper around a variety of logging API implementations

Math	Lightweight, self-contained mathematics and statistics components
Modeler	Mechanisms to create Model MBeans compatible with JMX specification
Net	Collection of network utilities and protocol implementations
Pool	Generic object pooling component.
Primitives	Smaller, faster and easier to work with types supporting Java primitive types
Proxy	Library for creating dynamic proxies
SCXML	An implementation of the State Chart XML specification aimed at creating and maintaining a Java SCXML engine. It is capable of executing a state machine defined using a SCXML document, and abstracts out the environment interfaces.
Validator	Framework to define validators and validation rules in an xml file
VFS	Virtual File System component for treating files, FTP, SMB, ZIP and such like as a single logical file system

FEA Categories

Service Area	Service Category	Service Standard Code
N/A	N/A	N/A

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Quartz Enterprise Job Scheduler related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (11/16/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	The versioning information for each of the Apache Commons components vary by component. Consumers should target the latest version available for each component.

General Analysis

Architectural Area

- Application

Architectural Benefits

- Apache Commons promotes source code reuse which can enhace productivity and reduce software errors.

Architectural Risks

- None significant.

EA Requirement

- ENTR 1074 - Implement a One VA information technology framework that supports the integration of information across business lines and that provides a source of consistent, reliable, accurate, and secure information to veterans and their families, employees, and stakeholders (Enabling Objective E-3).

Tier Used

- Other Tier

Tool Type

- Open Source

Tool Usage

- Development

General Assessment

Expected Usage:	Reusabla Java source code components.
Assessment Type:	New
Assessment Date:	11/19/2008
Notes:	The Apache Commons project differs from many other Apache hosted projects because it is comprised of multiple, independently released packages. Each component in the Commons collection is versioned and released independently.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	The Apache Commons collection of Java API's promotes source code reuse and has a good track record in HeV (CISS has been using Commons under waiver 08-074).

4.10) Apache Struts

General Information

Website:	http://struts.apache.org/
Description:	Apache Struts (formerly listed on the TRM as "Struts plus Tiles"), is a Java-based open source project sponsored by the Apache Software Foundation. The project is called “Struts” because the framework is meant to furnish the “invisible underpinnings” that support Web-based application development with Java. The Struts framework makes-up for the shortcomings of Java SE in thin-client and Web-based application development.

Struts has evolved into two distinct versions: Struts 1 and Struts 2. Struts versions 1.x are mature, widely documented, implemented, (in HeV applications) and supported. Struts 2 is a completely new approach based on the merger of the WebWork framework and Struts.

Decision: Approved

Decision Constraints:
- Projects deployed with Struts versions 1 should gradually migrate to the Spring framework as that transition is practicable.
- New projects in technology planning should use the Spring framework instead of Struts.
- Projects planning for the re-write of their applications to support Struts versions 2 should move to the Spring framework instead.

Decision Source: ARB

Decision Process: TRM v2

Decision Date: 9/17/2008

Current Status: Analysis Completed

Introduced By: Extended Tool List (ETL)

Vendor Name: ASF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	895: Middleware

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)

- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***
- Apache Commons - ***(required libraries)***

Comparable Technologies/Standards:

- Spring Framework

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.3.5	8/16/2006		
2.1.6	1/13/2009		
2.1.8	9/29/2009		
1.3.8	3/10/2007		
1.3.9	8/11/2007		
1.3.10	12/4/2008		
2.0.6	2/22/2007		
2.0.8	6/11/2007		
2.0.9	7/24/2007		
2.0.11	9/22/2007		
2.0.12	10/16/2008		

VA Forecast Information (10/14/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is

considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.3.5	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.3.8	Supported	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.3.9	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.3.10	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	**Version 2 of Struts is not approved for use.** The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment development and deployment of Struts is currently based on version 1.3.10.

General Analysis

Architectural Area

- Application

Architectural Benefits

- For projects already deployed on Struts, Struts 1 provides a reusable, standardized framework for producing Java applications using the Model View Controller design pattern.

Architectural Risks

- It appears that the Struts framework has reached the point where its innovation and adoption will begin to decline. Craig McClanahan, chief architect and author of Struts, has left the project for good--and he is urging current Struts users to migrate to newer Web frameworks.
- Struts is a Web (presentation) framework only; therefore by definition, the project will need to incorporate additional frameworks or Java-based helpers to complete an application. The use of multiple frameworks adds complexity and maintenance overhead.

Standards Traceability

- Java EE - EJB 3.0
- Java EE - JDBC 4.0

Tier Used

- Presentation Tier (Web)

Tool Type

- Framework

Tool Usage

- Development
- Management/Collaboration
- Runtime

General Assessment

Expected Usage:	A Model View Controller based framework for developing dynamic Web content with Java.
Assessment Type:	Refresh
Assessment Date:	12/23/2008
Notes:	Version 2 of the Apache Struts framework is a radical departure from version 1. Apache Struts 2 is in fact, the framework formerly known as WebWork. To change an application architecture from Struts 1 to Struts 2 will require a significant amount of rework time and resources. The advice of this analysis is to instead, use these resources to move to the Spring framework. The Spring framework contains all of the functionality found in Struts 1, as described here: **Struts Actions Are Spring Controllers** In Struts, Actions are core processing objects of the framework. They play the role of controllers in the MVC pattern. The Spring alternative to Struts Actions is the Controller interface. Spring Controllers process user input and dispatch to view components in Spring. The most significant differences between the Struts Action and the Spring Controller are that Actions are abstract classes and Controllers are interfaces. This design (also known as *design by interface*) minimizes the coupling between the application and the framework, and gives the architect greater flexibility in the design of the Controllers. With this in mind, the simplest intermediary transition step from Struts to Spring is to rewrite Actions so they implement the Controller interfaces and reuse the existing code. This allows incremental removal of all the Struts dependencies while keeping the application operational.

No Action Forms

One of the best things about the Spring framework is that it has no specialized ActionForm objects--Spring supports binding of HTTP form values directly into POJOs (Plain Old Java Objects). This feature greatly simplifies application maintenance by limiting the number of classes to create and maintain. A Struts ActionForm is not a true domain object--it is a place to hold user data until it can be validated and transferred into domain objects as commands. The advantage of the Struts ActionForm approach is that invalid data can be redisplayed easily; the disadvantage is that the data has to get into a domain object at some point, and Struts can only provide one-half of that solution. The Struts to Spring migration would mean dropping form beans and using domain objects directly--but this is not mandatory as it is still possible to use Form Bean objects as a map between the form inputs and domain objects.

ActionForwards versus ModelAndView

In Struts ActionMapping, objects are pointers into presentation resources (Actions, JSPs, Tiles, HTML files, etc.). The closest component in Spring MVC to ActionMapping is the ModelAndView interface. Spring Controllers return implementations of the ModelAndView interface, which like a Controller can be customized. Or, if appropriate, you can use the ModelAndView implementation supplied by Spring MVC. As the name implies, ModelAndView objects have Model and View components. Model components contain the business object to be displayed via the View component. Depending on the scenario, ModelAndView implementations may not have any Model components included. They may simply forward into some form of an actual View component (JSP, XSLT, Tiles, HTML, XML, etc.).

The migration from Struts 1 to Spring can be accomplished using one of the following strategies:

Strategy 1: Spring Enabling of Struts Components

For projects who want to migrate slowly, the first step is to enable Struts Actions as Spring Beans. This is a simple process, and the Spring documentation details it well. It does not require any changes to the existing Struts code, but it enables Struts Controller components, Actions, to be treated as Spring Beans. In this process, Actions inherit the nature of the Spring Beans and, therefore, start looking a lot like Spring Controllers.

Slow and step-wise migration is possible with this process. Each Action could be replaced one at a time by the Spring Controllers without rewriting the application at once and interrupting the existing page-flow sequences.

Strategy 2: Spring with Tiles
Another alternative, fully supported by the Spring framework, is to replace Struts Controllers and related components (Actions, Form Beans, etc.) with Spring MVC components while keeping Tiles as the pure "view" framework. Spring MVC does not have a specific alternative to Tiles, so architects may decide to keep their investments in Tiles and make them work through Spring MVC.
The one serious disadvantage of this approach is that you will effectively maintain two diverse Web frameworks in your Web application, which could result in a greater maintenance burden and training effort.
Strategy 3: Complete Migration
Complete migration would mean total replacement of all the components of the Struts framework with Struts MVC. At the end of the process, no Struts-specific components would remain in the application.

Recommendation: Approve-Conditional

Recommendation Constraints:

Recommendation Justification: The recommendation is to approve the continued use of Struts with conditions:

- Projects deployed with Struts versions 1 should gradually migrate to the Spring framework as that transition is practicable.
- New projects in technology planning should use the Spring framework instead of Struts.
- Projects planning for the re-write of their applications to support Struts versions 2 should move to the Spring framework instead.

Struts is a Web (presentation) framework only; therefore by definition, projects will need to incorporate additional frameworks or Java-based helpers to complete an application. The use of multiple frameworks adds complexity and maintenance overhead--so it is an architectural goal to reduce the number of frameworks used in the VA. In addition, Struts requires use of Struts-specific objects that couples the view (in the Model, View, Controller, or MVC pattern) to this particular technology. Another architectural goal is the separation of concerns so that any of the MVC elements can be changed without a major re-write of the application. Spring provides a MVC approach without any inherent dependencies to the framework.

4.11) Apache Tomcat

General Information

Website: http://tomcat.apache.org/

Description: Apache Tomcat is an open source software implementation of the Java Servlet and JavaServer Pages technologies. It provides a "pure Java" HTTP web server environment for Java code to run.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: CDCO Supported Architecture Components

Vendor Name: ASF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	871: Web Servers

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Hypertext Transfer Protocol (HTTP) related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5.5	8/31/2004		
6.0	12/1/2006		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
6.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.12) Application Oriented Sites

General Information

Description: These services build on the Data-Oriented services by providing the ability to process complex logic (including transactions) based on a client's request.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Design Pattern	The implementation of these services should follow the Model-View-Controller (MVC) design pattern where the controller follows the servlet specification, the view follows the JSP or XSLT specification, and the model conforms to the JavaBean or POJO specification

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	887: Dynamic Server-Side Display

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.13) Architecture for IP Address Allocation with CIDR

General Information

Website:	http://tools.ietf.org/html/rfc1518
Description:	Architecture for IP Address Allocation with CIDR provides an architecture and a plan for allocating IP addresses in the Internet.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 1518	9/1/1993		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 1518	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.14) Audit Services

General Information

Description: A system's audit trail is a collection of audit records containing data about security relevant events, i.e., attempted violations of the security policy and changes to the security state of the system. Audit services provide the meansto record the chronological set of related records that provide evidence of system activity.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description

Separation of Power		There shall be a separation of duties between security personnel who administer the access control function and those who administer the audit trail.
Training		Reviewers shall know what to look for to be effective in spotting unusual activity. They need to understand what normal activity looks like.
Audit Trail Reviews		• Develop guidelines that describe how frequently audit trails are reviewed and whether there arereview guidelines. • Application owners, data owners, system administrators, data processing function managers, andcomputer security managers should determine how much review of audit trail records is necessary, based on the importance of identifying unauthorized activities. • Design the system to allow audit trail function queries by user ID, terminal ID, application name,date and time, or some other set of parameters to run reports of selected information. This makes the Audit trail reviews easier and more efficient. • The appropriate system-level or application-level administrator should review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Audit Log Retention	Audit logs should be maintained for a retention period specified in the applicable security policy.
Audit Record	At a minimum, each audit record should include the following, if applicable: • The type of event • The date and time the event occurred • A success or failure indicator • The identity of the entity and/or operator that caused the event
Audit Actions	Actions taken as a result of these reviews should be documented.
ISO/IEC 10181-7	Security Audit and Alarms Framework
ISO/IEC 10164-8	Security Audit Trail Function

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.15) Basic Transition Mechanisms for IPv6 Hosts Routers

General Information

Website:	http://tools.ietf.org/html/rfc4213
Description:	Basic Transition Mechanisms for IPv6 Hosts Routers specifies IPv4 compatibility mechanisms that can be implemented by IPv6 hosts and routers. Two mechanisms are specified, dual stack and configured tunneling. Dual stack implies providing complete implementations of both versions of the Internet Protocol (IPv4 and IPv6), and configured tunneling provides a means to carry IPv6 packets over unmodified IPv4 routing infrastructures.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008

Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 4213	10/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 4213	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.16) Biometric Application Programming Interface (BioAPI)

General Information

Website: http://www.iso.org/iso/catalogue_detail.htm?csnumber=33922

Description: ISO/IEC 19784 (formerly ANSI INCITS 358): Biometric Application Programming Interface (BioAPI) provides a defined interface that allows a software application to communicate with (utilize the services of) one or more biometric technologies. It includes a high-level generic biometric authentication model suited to a broad range of biometrically enabled applications and to most forms of biometric technology. An architectural model is described which enables components of a biometric system to be provided by different vendors, and to interwork through fully-defined Application Programming Interfaces (APIs), corresponding Service Provider Interfaces (SPIs), and associated data structures. BioAPI covers the basic biometric functions of enrollment, verification and identification, and includes a database interface to allow an application to manage

the storage of biometric records.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
BioAPI specification	This document defines the interface that allows a software application to communicate with (utilize the services of) one or more biometric technologies.
Biometric archive function provider interface	This document defines the interface between a biometric service provider (BSP) and a biometric archive function provider (BAFP) for BioAPI.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	3/1/2000		
1.1 (ANSI/INCITS 358)	1/1/2002		
2.0 (ISO/IEC 19784)	1/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.1 (ANSI/INCITS 358)	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.17) Biometric Information Management and Security

General Information

Website:	http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+X9.84%3a2003
Description:	Biometric Information Management and Security for the Financial Services Industry specifies the minimum security requirements for effective management of biometric data. Within the scope of this Standard the following topics are addressed: Security for the collection, distribution, and processing, of biometric data, encompassing data integrity, authenticity, and non-repudiation; Management of biometric data across its life cycle comprised of the enrollment, transmission and storage, verification, identification, and termination processes; Usage of biometric technology, including one-to-one and one-to-many matching, for the identification and authentication of banking customers and employees; Application of biometric technology for internal and external, as well as logical and physical access control; Encapsulation of biometric data; Techniques for the secure transmission and storage of biometric data; Security of the physical hardware used throughout the biometric data life cycle; Techniques for integrity and privacy protection of biometric data.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ANSI

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2003	1/1/2003		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on

the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2003	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.18) Biometric Services

General Information

Description: Biometrics deals with the automated methods of authenticating or verifying an individual based upon a physical or behavioral characteristic.<br
Biometrics is the science and technology of measuring and statistically analyzing biological data. Biometrics usually refers to technologies for measuring and analyzing human body characteristics such as fingerprints, eyeretinas and irises, voice patterns, facial patterns, and hand measurements, especially for authentication purposes.

Fingerprint and other biometric devices consist of a reader or scanning device, software that converts the scannedinformation into digital form, and wherever the data is to be analyzed, a database that stores the biometric data for comparison with previous records. When converting the biometric input, the software identifies specific points of data as match points. The match points are processed using an algorithm into a value that can be compared with biometric data scanned when a user tries to gain access.

Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
NIST FIPS 48	Guidelines On Evaluation Of Techniques For Automated Personal Identification
NIST FIPS 190	Guideline For The Use Of Advanced Authentication Technology Alternatives
CDSA/CSSM Authentication: HRS API	Common Data Security Architecture (CDSA)/Common Security Services Manager (CSSM) Authentication: Human Recognition Service (HRS) API
ISO/IEC 7816-11	Personal Verification Through Biometric Methods

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.19) BMC Mainview

General Information

Website:	http://www.bmc.com/products/brand/mainview.html
Description:	BMC Mainview provides historical performance monitoring in a single mainframe solution that integrates across z/OS, z/VM, Linux, and subsystems.
Decision:	Approved
Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	BMC Software

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	Network Management Services*

Operating Systems Supported

- Red Hat Linux
- z/OS
- z/VM

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- BMC Performance Manager
- Wily Introscope
- Strobe

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2.8			
2.9	8/1/2008		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2.8	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.20) Border Gateway Protocol (BGP)

General Information

Website: http://tools.ietf.org/html/rfc4271

Description: Border Gateway Protocol (BGP) defines an inter-autonomous system routing protocol for the Internet.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 1771	3/1/1995		
RFC 4271	1/1/2006		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 4271	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.21) Broadband Audiovisual Communication Systems and Terminals

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=H

Description: ITU-T H.310: Broadband Audiovisual Communication Systems and Terminals covers the technical requirements for the systems and terminals of broadband audiovisual communication services defined in H.200/AV.100-series Recommendations. Both H.310 unidirectional and bidirectional broadband audiovisual terminals are defined. The classification of H.310 terminals into different terminal types is based on a set of audiovisual, network adaptation, and signalling capabilities. With these capabilities, H.310 terminals support a wide range of conversational and distributive applications and services. This revision enhances the interworking between different type of H.310 terminals.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2	9/25/1998		

2.1	1/8/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2.1	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.22) Call Signalling Protocols and Media Stream Packetization

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=H

Description: ITU-T H.225: Call signalling protocols and media stream packetization for packet-based multimedia communication systems covers the technical requirements for narrow-band visual telephone services defined in ITU-T H.200 and F.720-series Recommendations, in those situations where the transmission path includes one or more packet-based networks, each of which is configured and managed to provide a non-guaranteed Quality of Service (QoS) which is not equivalent to that of N-ISDN, such that additional protection or recovery mechanisms beyond those mandated by ITU-T Rec. H.320 need be provided in the terminals. It

is noted that ITU-T Rec. H.322 addresses the use of some other LANs which are able to provide the underlying performance not assumed by the ITU-T Recs H.323 and H.225.0.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5	7/14/2003		
6	5/29/2005		
6.1	1/13/2007		
7	12/14/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
6	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.23) Carrier Sense Multiple Access with Collision Detection

(CSMA/CD)

General Information

Website: http://standards.ieee.org/getieee802/802.3.html

Description: IEEE 802.3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications - Ethernet local area network operation is specified for selected speeds of operation from 1 Mb/s to 10 Gb/s using a common media access control (MAC) specification and management information base (MIB). The Carrier Sense Multiple Access with Collision Detection (CSMA/CD) MAC protocol specifies shared medium (half duplex) operation, as well as full duplex operation. Speed specific Media Independent Interfaces (MIIs) allow use of selected Physical Layer devices (PHY) for operation over coaxial, twisted pair or fiber optic cables. System considerations for multisegment shared access networks describe the use of Repeaters which are defined for operational speeds up to 1000 Mb/s. Local Area Network (LAN) operation is supported at all speeds. This specification includes:

- 100 Mb/s baseband network, type 100BASE-T
- 1000 Mb/s baseband network
- 10Gb/s baseband network
- Ethernet for subscriber access networks

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IEEE

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	Campus Area Network (CAN)*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2005	1/1/2005		
2008	1/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is

considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2005	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.24) Cascading Style Sheets (CSS)

General Information

Website: http://www.w3.org/TR/CSS2/

Description: Cascading Style Sheets (CSS) is a style sheet language that allows authors and users to attach style (e.g., fonts and spacing) to structured documents (e.g., HTML documents and XML applications). By separating the presentation style of documents from the content of documents, CSS simplifies Web authoring and site maintenance.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	888: Content Rendering

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2	5/12/1998		
2.1	9/8/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the

responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
2.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.25) Cascading Style Sheets Mobile Profile (CSS-Mobile)

General Information

Website: http://www.w3.org/TR/css-mobile/

Description: This specification defines in general a subset of CSS that is to be considered a baseline for interoperability between implementations of CSS on constrained devices (e.g. mobile phones). Its intent is not to produce a profile of CSS incompatible with the complete specification, but rather to ensure that implementations that due to platform limitations cannot support the entire specification implement a common subset that is interoperable not only amongst constrained implementations but also with complete ones.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008
Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	888: Content Rendering
Service Platform and Infrastructure	Support Platform	864: Wireless / Mobile

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Cascading Style Sheets (CSS) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2.0	12/10/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.26) Checksum Hash Value

General Information

Description: A checksum or hash value is used to detect errors or manipulation during transmission.

A checksum is a count of the number of bits in a transmission unit that is included with the unit so that the receivercan check to see whether the same number of bits arrived. If the counts match, it's assumed that the complete transmission was received. Both TCP and UDP communication layers provide a checksum count and verification as one of their services.

	Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. The hashing algorithm is called the hash function. A good hash function should not produce the same hash value from two different inputs. In this manner, comparison of hash values can be used to verify the integrity of a data file or element.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
NIST FIPS 113	Computer Data Authentication
NIST SP 500-156	Message Authentication Code (MAC) Validation System: Requirements and Procedures
NIST SP 800-21	Guideline for Implementing Cryptography in the Federal Government
NIST SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
NSA - Network Security Guide	The 60 Minute Network Security Guide

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.27) Classless Inter-Domain Routing (CIDR)

General Information

Website:	http://tools.ietf.org/html/rfc4632
Description:	Classless Inter-Domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan discusses the strategy for address assignment of the existing 32-bit IPv4 address space with a view toward conserving the address space and limiting the growth rate of global routing state.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 1519	9/1/1993		
RFC 4632	8/1/2006		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or

production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 4632	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.28) Coding of Speech Using Low-Delay Code Excited Linear Prediction

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=G

Description: ITU-T G.728: Coding of Speech at 16 kbit/s Using Low-Delay Code Excited Linear Prediction contains the description of an algorithm for the coding of speech signals at 16 kbit/s using low-delay code excited linear prediction (LD-CELP).

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.8	2/17/2000		
1.9	5/29/2006		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.9	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.29) Common Biometric Exchange Formats Framework (CBEFF)

General Information

Website: http://csrc.nist.gov/publications/PubsNISTIRs.html

Description: NIST IR 6529 A: Common Biometric Exchange formats Framework (CBEFF) describes a set of data elements necessary to support biometric technologies in a common way. These data elements can be placed in a single file used to exchange biometric information between different system components or between systems. The result promotes interoperability of biometric-based application programs and systems developed by different vendors by allowing biometric data interchange.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	NIST

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
6529-A	4/5/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.30) Common Language Infrastructure (CLI)

General Information

Website: http://www.ecma-international.org/publications/standards/Ecma-335.htm

Description: ISO/IEC 23271 & ECMA-332: This standard defines the Common Language Infrastructure (CLI) in which applications written in multiple high-level languages can be executed in different system environments without the need to rewrite those applications to take into consideration the unique characteristics of those environments.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision EA

Source:	
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ECMA

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Technical Report on Information Derived from Partition IV XML File	

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
4	6/1/2010		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
4	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.31) Common Object Request Broker Architecture (CORBA)

General Information

Website: http://www.omg.org/technology/documents/corba_spec_catalog.htm

Description: Common Object Request Broker Architecture (CORBA) is a vendor-independent architecture and infrastructure that computer

applications use to work together over networks. Using the standard protocol IIOP, a CORBA-based program from any vendor, on almost any computer, operating system, programming language, and network, can interoperate with a CORBA-based program from the same or another vendor, on almost any other computer, operating system, programming language, and network.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: OASIS

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Interfaces	This document specifies the CORBA Object Model and uses concepts from that model to define the operation of the Object Request Broker (ORB). The ORB is the basic mechanism by which objects transparently make requests to - and receive responses from - each other on the same machine or across a network.
Interoperability	This document specifies a comprehensive, flexible approach to supporting networks of objects that are distributed across and managed by multiple, heterogeneous CORBA-compliant Object Request Brokers (ORBs).
Components	This specification defines: • The syntax and semantics of a component model • A language to describe the structure and state of component implementations • A programming model for constructing component implementations

	• A runtime environment for component implementations • Interaction between components and Enterprise Java Beans • Meta-data for describing component-based applications, and interfaces for their deployment • A lightweight subset of the component model, programming model and runtime environment)

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	895: Middleware

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.0	6/2/2001		
3.1	4/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the

responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
3.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.32) Common Warehouse Metamodel (CWM)

General Information

Website: http://www.omg.org/technology/documents/modeling_spec_catalog.htm

Description: The Common Warehouse Metamodel (CWM) defines interfaces that can be used to enable easy interchange of warehouse and business intelligence metadata between warehouse tools, warehouse platforms and warehouse metadata repositories in distributed heterogeneous environments.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: OMG

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Database/Storage	Warehouse Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.1	3/2/2003		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.33) Computer Based Training Exchange

General Information

Description:	Computer Based Training (CBT) Exchange standards support the development, deployment, and interoperability of CBT and Learning systems.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
AICC AGR006 - Computer Managed Instruction (CMI)	This document recommends guidelines that promote the interoperability of CMI systems.
AICC AGR010 - Web-based Computer Managed Instruction (CMI)	This document recommends guidelines that promote the interoperability of Web-Based CMI systems.
AICC CMI001 - AICC/CMI Guidelines For Interoperability	This document defines the following: • The mechanism used by the CMI to launch CBT content • Common mechanisms and data for CMI/CBT communication • A common definition for organization and sequencing of CBT content in a course

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.34) Computer Graphics Metafile (CGM)

General Information

Website: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

Description: The Computer Graphics Metafile provides a file format suitable for the storage and retrieval of picture information. The file format consists of a set of elements that can be used to describe pictures in a way that is compatible between systems of different architectures and devices of differing capabilities and design. This picture description includes the capability for describing static pictures. Static pictures are those where elements which may lead to dynamic effects (for example those leading to regeneration) are prohibited within the picture body.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Functional specification	

Binary encoding	

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	888: Content Rendering

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1999	12/15/1999		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010	CY2011	CY2012

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1999	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.35) Confidentiality Framework

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=24329

Description: ISO/IEC 10181-5: The Information technology - Open Systems Interconnection - Security frameworks for open systems: Confidentiality framework specifies a general framework for the provision of confidentiality services.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1996	1/1/1996		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1996	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.36) Confidentiality Services

General Information

Description: Confidentiality refers to keeping electronic data private; i.e., preventing unauthorized individuals or processes fromgaining access to documents, transactions, data, or messages. Confidentiality services ensure that data is notmade available or disclosed to unauthorized individuals or computer processes. This is accomplished through theuse of data encryption, security association, and key management. In addition, these services ensure thatobservation of usage patterns of communications resources is not possible.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Scope		Confidentiality services shall be applied to devices that permit human interaction with the information system.
SSL		Servers that use SSL shall be configured to enable SSL only.
Certification		All software and hardware providing encryption services shall be certified according to the FIPS 140 - Security Requirements for Cryptographic Modules standards.
Data Storage Encryption Algorithm		Data at rest encryption shall employ products that use the symmetric data encryption algorithm AES

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
E-mail Encryption	E-mail encryption should be deployed as S/MIME based solutions. PKI supports trusted digital signatures in S/MIME messages and should be utilized to implement e-mail encryption.
ISO/IEC 10181-4	Non-repudiation Framework

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	885: Supporting Security Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.37) Configuration Management

General Information

Description: Configuration management is the management of system change. Configuration management includes procedures for change control, system and network building, network baselining, auditing, and version management. Configuration management establishes change control. The challenge of change is that a change to the network is likely to introduce new faults or expose other faults that had not been observed prior to the change. Change control procedures ensure that the changes to a system are made in a controlled way so that their effect on the system can be predicted. Version management refers to keeping track of the version of operating systems running on the network devices.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Network Management		The network management system shall display management data, monitor and control managed devices, and communicate with management agents. Data link and physical layer parameters shall be monitored by management systems that are based on Management Information Base (MIB) - Remote Monitoring (RMON) standards.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Configuation Management Database	A configuration management database should be used to house information about network configurations. When a network is operational, it is important that changes be implemented using a controlled methodology.
Management Device	A router, server, switch, or end system should be selected on each network to be a local management device.
Configuration Management	After a configuration is verified and validated, it should be stored for future reference

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	Network Management Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.38) Control Protocol for Multimedia Communication

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=H

Description: ITU-T H.245: Control Protocol for Multimedia Communication specifies syntax and semantics of terminal information messages as well as procedures to use them for in-band negotiation at the start of or during communication. The messages cover receiving and

transmitting capabilities as well as mode preference from the receiving end, logical channel signalling, and Control & Indication. Acknowledged signalling procedures are specified to ensure reliable audiovisual and data communication.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
12	10/7/2005		
13	5/29/2006		
14	6/13/2008		
15	12/14/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
13	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.39) Cryptographic Algorithm Implementation Requirements

for ESP and AH

General Information

Website: http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

Description: The IPsec series of protocols makes use of various cryptographic algorithms in order to provide security services. The Encapsulating Security Payload (ESP) and the Authentication Header (AH) provide two mechanisms for protecting data being sent over an IPsec Security Association (SA). To ensure interoperability between disparate implementations, it is necessary to specify a set of mandatory-to-implement algorithms to ensure that there is at least one algorithm that all implementations will have available. Cryptographic Algorithm Implementation Requirements for ESP and AH defines the current set of mandatory-to-implement algorithms for ESP and AH as well as specifying algorithms that should be implemented because they may be promoted to mandatory at some future time.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code

Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 4305	12/1/2005		
RFC 4835	4/1/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
RFC 4305	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

Forecast Note:	

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.40) Data Center

General Information

Refer to document:	VA_Data_Center_Standards_1_0.pdf
Description:	This standards document lists the acceptable and recommended specifications for Data Center passive Inside Plant, including racks, equipment enclosures, fiber and copper transport media, KVM, and rack-level power distribution. Sections include standard specifications for subject components, decisions supporting the standard specifications, guidelines or recommendations for implementing the standard specifications, and supplemental factors to consider when evaluating subject components. Other supplementary documents will provide guidance on procuring components that meet the standard specifications, guidance on integrating them with existing components, and explanation of how the subject components fit into the VA Architecture. This standard includes the following: Support Infrastructure (Equipment Enclosure; Open Rack; Cable Tray; Horizontal Cable Management Panels; Vertical Cable management Panels; Fiber Distribution Cabinets); Transport Media and Interfaces (Patch Panels; Fiber Distribution Cassettes; UTP; Fiber Optic Cable; UTP Patch Cords; Fiber Patch Cords); Enclosure Power Distribution (Power Distribution Units; Zone Power Distribution Units); Remote Management Technology (KVM).
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EIE CTO
Decision	TAR-TAS

Process:
Decision Date: 11/13/2009
Current Status: Analysis Completed
Introduced By: OPS/EIE

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Requirements	861: Hosting

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date

Vendor release information is not available for this entry.

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.41) Data Encryption Standard (DES)

General Information

Website: http://csrc.nist.gov/publications/PubsFIPSArch.html

Description: Data Encryption Standard (DES) specifies two cryptographic algorithms, the DES algorithm and the Triple Data Encryption Algorithm (TDEA) which may be used by Federal organizations to protect sensitive data. Protection of data during transmission or while in storage may be necessary to maintain the confidentiality and integrity of the information represented by the data. The algorithms uniquely define the mathematical steps required to transform data into a cryptographic cipher and also to transform the cipher back to the original form.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	NIST

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
FIPS 46-3	10/1/1999		5/19/2005

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
FIPS 46-3	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.42) Data Format Classification

General Information

Description: Defines the structure of a file. There are hundreds of formats, and every application has many different variations (database, word processing, graphics, executable program, etc.). Each format defines its own layout of the data.The file format for text is the simplest.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Procedures for Establishing & Managing Privacy Act Systems of Records	VA Handbook 6300.5	This handbook sets forth procedures for establishing and managing systems of records under the Privacy Act.
Records & Information Management	VA Directive 6300	This directive provides policy for the Department of Veterans Affairs (VA) Records Management (RM) program, which includes records management, micrographics management, vital records, the Privacy Act (PA), the Freedom of Information Act (FOIA), the Computer Matching and Privacy Protection Act, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Release of Names and Addresses (RONA).
VistA Lexicon Utility		

Guidelines and Best Practices

No guidelines have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.43) Data Format for Fingerprint, Facial, & SMT Information

General Information

Website:	http://www.itl.nist.gov/ANSIASD/sp500-245-a16.pdf
Description:	ANSI/NIST-ITL: Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information defines the content, format, and units of measurement for the exchange of fingerprint, palmprint, facial/mugshot, and scar, mark, & tattoo (SMT) image information that may be used in the identification process of a subject. The information consists of a variety of mandatory and optional items, including scanning parameters, related descriptive and record data, digitized fingerprint information, and compressed or uncompressed images.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	NIST

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Data Format for the Interchange of Fingerprint. Part 2: XML Version	
Data Format for the Interchange of Fingerprint. Part 1	

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2000	7/27/2000		
2007	4/20/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2000	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.44) Data Integrity

General Information

Description: Data integrity is the condition where data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.
Integrity, in terms of data and network security, is the assurance that information can only be modified by those authorized to do so. Measures taken to ensure integrity include controlling the physical environment of networked terminals and servers, restricting access to data, and maintaining rigorous identification, authentication, and

authorization practices. Data integrity can also be threatened by environmental hazards, such as heat, dust, water, and electrical surges.
Practices followed to protect data integrity in the physical environment include: making servers accessible only to network administrators; keeping transmission media (such as cables and connectors) covered and protected to ensure that they cannot be tapped; and protecting hardware and storage media from power surges, electrostatic discharges, and magnetism.
Network administration measures to ensure data integrity include: maintaining current authorization levels for all users, documenting system administration procedures, parameters, and maintenance activities, and creating disaster recovery plans for occurrences such as power outages, server failure, and virus attacks.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
NIST FIPS 113	Computer Data Authentication
NIST SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
NSA - Network Security Guide	The 60 Minute Network Security Guide

FEA Categories

Service Area	Service Category	Service Standard Code

Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.45) Data Oriented Sites

General Information

Description:	These services provide the ability to interact with a data repository based on a client's request. Typically, these services are used to dynamically generate a site's content or to enter a user's non-transactional input into a database. However, the logic associated with this service should be limited to data validation, database retrieval SQL, or "gluing" component logic together.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Encapsulation	Encapsulate logic in either servlets or JavaBeans. Avoid putting processing logic directly in JSPs.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	887: Dynamic Server-Side Display

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.46) Data Protocols for Multimedia Conferencing

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=T

Description: ITU-T T.120: Data Protocols for Multimedia Conferencing define a multipoint data communication service for use in multimedia conferencing environments. The purpose of ITU-T T.120 is to provide an introduction and guide to the T.120 series. ITU-T T.120 defines the T.120 architectural model and shows the interrelationships between the constituent Recommendations.

Decision: Approved

Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1	7/3/1996		
1.1	2/6/1998		
2	1/13/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.47) Data Protocols for Multimedia Conferencing - Generic Conference Control

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=T

Description: ITU-T T.124: Data Protocols for Multimedia Conferencing - Generic Conference Control rovides a high-level framework for conference management and control of multimedia terminals and Multipoint Control Units (MCUs). It encompasses Generic Conference Control (GCC) functions such as conference establishment and termination, managing the roster of terminals participating in a conference, managing the roster of applications and application capabilities within a conference, registry services for use by applications, coordination of conference conductorship, as well as other miscellaneous functions. It depends on companion Recommendations T.122 and T.125 (MCS) and T.123 as part of the T.120 infrastructure.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2	2/6/1998		
3	1/13/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.48) Database Services

General Information

Description: Refers to a collection of information organized in such a way that a computer program can quickly select desired pieces of data. A database management system (DBMS) is a software application providing management, administration, performance, and analysis tools for databases.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Relational		Enterprise-level data shall be stored using a relational model toenforce referential integrity.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
High Availability	Enterprise-level data needing 24/7-availability under COOP should be automatically replicated across multiple data centers.
Data Services	Component services are the preferred access method to enterprise-level data especially when dealing with updateable transactions.

Normalization	Third Normal Form (3NF) is the preferred minimal normalization standard for all data.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Database/Storage	875: Database

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.49) Datatypes for DTDs (DT4DTD)

General Information

Website:	http://www.w3.org/TR/dt4dtd
Description:	Datatypes for DTDs (DT4DTD) allows legacy systems that may presently be unable to convert their DTD markup declarations to XML Schema, to utilize XML Schema conformant datatypes. With it, DTD creators can specify datatypes for attribute values and data content, thereby providing the foundation for a smoother future transition path.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2

Decision Date: 3/14/2008
Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	898: Data Types / Validation

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Extensible Markup Language (XML) - Standard
- XML Schema - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	1/13/2000		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.50) Differentiated Services (DS) Field in IPv4 and IPv6 Headers

General Information

Website: http://tools.ietf.org/html/rfc2474

Description: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers defines the IP header field, called the DS (for differentiated services) field. In IPv4, it defines the layout of the TOS octet; in IPv6, the Traffic Class octet. In addition, a base set of packet forwarding treatments, or per-hop behaviors, is defined.

Decision: Approved

Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2474	12/1/1998		
RFC 3168	9/1/2001		
RFC 3260	4/1/2002		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2474	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.51) Digital Compression and Coding of Continuous-Tone Still Images

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18902

Description: ISO/IEC 10918-1 & ITU-T T.81: Digital Compression and Coding of Continuous-Tone Still Images – Requirements and Guidelines specifies processes for converting source image data to compressed image data, processes for converting compressed image data to reconstructed image data, coded representations for compressed image data, and gives guidance on how to implement these processes in practice. Is applicable to continuous-tone - grayscale or colour - digital still image data and to a wide range of applications which require use of compressed images. Is not applicable to bi-level image data.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1	9/18/1992		
1.1	1/30/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.52) Digital Signature

General Information

Description: A Digital Signature is a Cryptographic process used to assure message originator authenticity, integrity, and non-repudiation.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
NIST SP 800-2	Public-Key Cryptography
NIST SP 800-21	Guideline for Implementing Cryptography in the Federal Government
NIST SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.53) Digital Signature Standard (DSS)

General Information

Website:	http://csrc.nist.gov/publications/PubsFIPS.html
Description:	FIPS 186: Digital Signature Standard (DSS) specifies a suite of algorithms that can be used to generate a digital signature. Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation, since the signatory cannot easily repudiate the signature at a later time.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	NIST

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	884: Certificates / Digital Signature

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2	1/1/2000		6/10/2009
3	6/10/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.54) Dimensions CM

General Information

Website: http://www.serena.com/products/Dimensions-cm-configuration-management/

Description: Dimensions CM is a software configuration management solution that supports parallel and geographically distributed development.

Decision: Approved

Decision Constraints: Dimensions is approved for Benefits products only with the concurrence of SIO and Tools Management.

Decision Source: Benefits Arch

Decision Process: TRM v4.1

Decision Date: 10/28/2009

Current Status: Pending Analysis

Introduced By: Benefits ASA

Vendor Name: Serena Software

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	868: Software Configuration Management

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***
- Eclipse - ***(required libraries)***

Comparable Technologies/Standards:

- Rational ClearCase with MultiSite

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
9.1	11/5/2004		
10.1	9/15/2006		

VA Forecast Information (09/28/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
10.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.55) Directory Server

General Information

Website: http://www.sun.com/software/products/directory_srvr_ee/dir_srvr/index.xml

Description: The Directory Server, formerly known as the Sun Java System Directory Server, is a scalable LDAP data store for identity information.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center

	Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	Oracle

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Simple Object Access Protocol (SOAP) related as: (Companion)
- Lightweight Directory Access Protocol (LDAP) related as: (Companion)
- Hypertext Transfer Protocol (HTTP) related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5.2	6/6/2003		
6.0	3/1/2007		
6.2	9/1/2007		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
6.2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.56) Discovery Services

General Information

Description: Directory services help people and applications find the names and addresses of objects and services available to an application. Directory services implemented across an enterprise enable people to find destination recipients in other organizations. Directory services can be connected to the entire VA and can store information such as names of users; organizations; network resources; mailbox addresses; and message distribution lists. Interoperability among external computer systems is supported through compliance with international directory services and standards protocols.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
LDAP		Directory Services shall run a native Lightweight Directory Services Protocol (LDAP) Directory Server running directly over TCP to a database acting as a backend to another server.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Applicability	The Directory can be used as a repository for many kinds of information. The full power of DAP is unnecessary for applications that require simple read access to a few attribute values. Applications addressing is a good example of this type of use where an application entity needs to determine the Presentation Address (PA) of a peer entity given that peer's Application Entity Title (AET). If the AET is a Directory Name (DN), then

	the required result can be obtained from the PA attribute of the Directory entry as identified by the AET. This is very similar to DNS.
LDAP vs. X.500	LDAP is preferred to full X.500 services.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	Discovery Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.57) Diskeeper

General Information

Website:	http://www.diskeeper.com/diskeeper/diskeeper.aspx
Description:	Diskeeper is a file system defragmenter.
Decision:	Approved
Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed

Introduced By: CDCO Supported Architecture Components
Vendor Name: Diskeeper Corp.

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Business Logic	891: Platform Dependent Technologies

Operating Systems Supported

- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2007			

2008			
2009			
2010			

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2008	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.58) Domain Name Service

General Information

Description: The VA requires a mechanism that maps domain names to IP addresses for end systems to communicate easily within the VA network. The Domain Name Service (DNS) allows network devices to be identified and configured with a descriptive domain name.

Network resources like routers, servers, and workstations can be identified with a host name, instead of an IP address. Domain names are part of the machine name used in e-mail addresses and in host names. DNS maps host names and domain names to IP addresses. Since domain names are alphabetic, they are easier to

remember. The conversion from domain name to IP addresses is essential because the computer needs to process numeric information to complete the transaction.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Configuration	Configure DNS within the operating system or application residing at the middleware layer.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	Domain Name Service*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.59) Domain Name System (DNS) Configuration Options

General Information

Website:	http://tools.ietf.org/html/rfc3646
Description:	DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6) describes options for passing a list of available DNS recursive name servers and a domain search list to a client.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3646	12/1/2003		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 3646	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.60) Domain Name System (DNS) Extensions

General Information

Website:	http://tools.ietf.org/html/rfc3596
Description:	Domain Name System (DNS) Extensions to Support IP Version 6 (IPv6) defines the changes that need to be made to the Domain Name System (DNS) to support hosts running IP version 6 (IPv6). The changes include a resource record type to store an IPv6 address, a domain to support lookups based on an IPv6 address, and updated definitions of existing query types that return Internet addresses as part of additional section processing. The extensions are designed to be compatible with existing applications and, in particular, DNS implementations themselves.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	Domain Name Service*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3596	10/1/2003		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

RFC 3596	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.61) Domain Name System (DNS) Structure and Delegation

General Information

Website: http://tools.ietf.org/html/rfc1591

Description: Domain Name System Structure and Delegation provides some information on the structure of the names in the Domain Name System (DNS), specifically the top-level domain names; and on the administration of domains. The Internet Assigned Numbers Authority (IANA) is the overall authority for the IP Addresses, the Domain Names, and many other parameters, used in the Internet. The day-to-day responsibility for the assignment of IP Addresses, Autonomous System Numbers, and most top and second level Domain Names are handled by the Internet Registry (IR) and regional registries.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	Domain Name Service*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 1591	3/1/1994		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be

supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 1591	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.62) Dynamic Host Configuration Protocol (DHCP)

General Information

Website: http://tools.ietf.org/html/rfc2131

Description: The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCPIP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options. DHCP captures the behavior of BOOTP relay agents, and DHCP participants can interoperate with BOOTP participants.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2131	3/1/1997		
RFC 3396	11/1/2002		
RFC 4361	2/1/2006		

RFC 5494	4/1/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
RFC 2131	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.63) Dynamic Host Configuration Protocol Configuration of IPsec Tunnel Mode (DHCPv4)

General Information

Website: http://tools.ietf.org/html/rfc3456

Description: Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode explores the requirements for host configuration in IPsec tunnel mode, and describes how the Dynamic Host Configuration Protocol (DHCPv4) may be leveraged for configuration. In many remote access scenarios, a mechanism for making the remote host appear to be present on the local corporate network is quite useful. This may be accomplished by assigning the host a "virtual" address from the corporate network, and then tunneling traffic via IPsec from the host's ISP-assigned address to the corporate security gateway. In IPv4, DHCP provides for such

remote host configuration.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3456	1/1/2003		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 3456	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.64) Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

General Information

Website: http://tools.ietf.org/html/rfc3315

Description: The Dynamic Host Configuration Protocol (DHCP) for IPv6 enables DHCP servers to pass configuration parameters such as IPv6

network addresses to IPv6 nodes. It offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3315	7/1/2003		
RFC 4361	2/1/2006		
RFC 5494	4/1/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 3315	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.65) Dynamic Server Side Display

General Information

Description: This consists of the software that is used to create graphical user interfaces with the ability to change while the program is running.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Network Delivered Applications - ActiveX controls		Web browsers shall not be permitted to download untrusted ActiveX controls that can access or modify resources (external to the browser) of the local machine.
Network Delivered Applications - applets		Web browsers shall not be permitted to download unsigned applets that can access or modify resources (external to the browser) of the local machine.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Simple interactions	JavaScript should be used for relatively simple interactions (i.e. forms validation, interactive menus, etc.)
Network delivered applications	Java applets should be used for complex network delivered applications.
Platform independence	Web based client-side services should be used unless their interactive capabilities are too restrictive for a particular application.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	887: Dynamic Server-Side Display

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.66) Dynamic Updates in the Domain Name System (DNS UPDATE)

General Information

Website: http://tools.ietf.org/html/rfc2136

Description: The Domain Name System was originally designed to support queries of a statically configured database. While the data was expected to change, the frequency of those changes was expected to be fairly low, and all updates were made as external edits to a zone's Master File.

Using this specification of the UPDATE opcode, it is possible to add or delete RRs or RRsets from a specified zone. Prerequisites are specified separately from update operations, and can specify a dependency upon either the previous existence or nonexistence of an RRset, or the existence of a single RR.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	Domain Name Service*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2136	4/1/1997		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2136	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.67) ebXML Collaboration Protocol Profile and Agreement (ebXML CPPA)

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39972

Description: ISO/TS 15000-1 & OASIS: ebXML Collaboration Protocol Profile and Agreement (ebXML CPPA) specifies the requirements for a collaboration-protocol profile (CPP), and a collaboration-protocol agreement (CPA). The CPP describes a trading partner's technical capabilities for performing electronic business. The CPA describes the agreement between two trading partners on the technical

	capabilities they will use for a specific electronic-business collaboration.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- ebXML Messaging Service (ebMS) - Standard
- Uniform Resource Identifiers (URI) - Standard
- Security Assertion Markup Language (SAML) - Standard
- Extensible Markup Language (XML) - Standard
- XML Namespaces (XML-NS) - Standard
- XML Schema - Standard
- XML Pointer Framework - Standard
- XLink - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2004	1/1/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2004	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.68) ebXML Messaging Service (ebMS)

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39973

Description: ISO/TS 15000-2 & OASIS: ebXML Messaging Service (ebMS) addresses the requirements for an ebXML message service handler for the eBusiness community. ebMS defines a communications-protocol neutral method for exchanging electronic business messages and defines specific enveloping constructs supporting reliable, secure delivery of business information. ebMS includes a flexible enveloping technique permitting messages that is independent of the payload, the communications protocol used, and also of any format type.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Core Features 3.0	This document is the specification of the core features of ebMS.
Conformance Profiles 3.0	This document is a non-normative supplement to the ebMS specification. It defines some conformance profiles that support specific messaging

	styles or context of use.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- WS-Reliable Messaging

Companion Technologies/Standards:

- Simple Object Access Protocol (SOAP) - Standard
- WS-Security - Standard
- Extensible Markup Language (XML) - Standard
- Uniform Resource Identifiers (URI) - Standard
- XML Namespaces (XML-NS) - Standard
- XML Schema - Standard
- XML Path Language (XPath) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2.0	4/1/2002		
3.0	7/12/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the

responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
3.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.69) ebXML Registry Information Model (ebRIM)

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39974

Description: ISO/TS 15000-3 & OASIS: The ebXML Registry Information Model (ebRIM) defines the requirements for the information model for the ebXML registry. The ebXML registry describes objects that reside in a repository for storage and safekeeping. The information model does not deal with the actual content of the repository. All elements of the information model represent metadata about the content stored in the repository. Such information is used to facilitate ebXML-based Business-to-Business partnerships and transactions. The registry information model provides a high-level schema for the ebXML registry. It provides information on the type of metadata that are stored in the registry as well as the relationships among metadata classes. The registry information model defines what types of objects are stored and defines how stored objects are organized. The abstract registry is implemented using one or both of the following concrete bindings: a SOAP binding using the HTTP protocol, or an ebXML messaging service binding. These specifications are compatible with other ebXML specifications.

Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interface	900: Service Discovery

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- ebXML Registry Services (ebRS) - Standard
- ebXML Collaboration Protocol Profile and Agreement (ebXML CPPA) - Standard

- XML Path Language (XPath) - Standard
- XML Namespaces (XML-NS) - Standard
- Extensible Markup Language (XML) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2004	1/1/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2004	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.70) ebXML Registry Services (ebRS)

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.h

tm?csnumber=39975

Description: ISO/TS 15000-4 & OASIS: Electronic business eXtensible Markup Language Registry services (ebRS) defines the interface between the registry and the registry clients, as well as the interaction protocols, message definitions and XML schema.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
ebXML Registry Services and Protocols	This document defines the services and protocols for an ebXML Registry.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interface	900: Service Discovery

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Universal Description, Discovery, and Integration (UDDI)

Companion Technologies/Standards:

- Extensible Markup Language (XML) - Standard
- Security Assertion Markup Language (SAML) - Standard
- Simple Object Access Protocol (SOAP) - Standard
- Structured Query Language (SQL) - Standard
- WS-I Basic Profile - Standard
- XML Path Language (XPath) - Standard
- XML Namespaces (XML-NS) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2004	1/1/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2004	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.71) Eclipse

General Information

Website:	http://www.eclipse.org
Description:	Eclipse is an open source (supported by IBM) integrated development environment composed of frameworks and common services. Plug-ins must be loaded, integrated and executed in order to equip Eclipse to handle Java software development. Eclipse is an open framework that has uses beyond that of a Java development environment. Eclipse forms the foundation for the Rational development tools offered by Enterprise Tools Management. The Rational tools should be utilized unless there is a compelling reason to deviate from the standard.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	Eclipse

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	867: Integrated Development Environments (IDE)

Operating Systems Supported

- Red Hat Linux
- Windows (Client)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***
- XSL Transformations (XSLT) - ***(required for some configurations)***

Comparable Technologies/Standards:

- Rational Software Architect
- MyEclipse
- Rational Systems Developer
- Rational Application Developer

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.2	6/30/2006		
3.3	6/29/2007		
3.4	6/25/2008		
3.5	6/24/2009		

3.6 (est)	6/30/2010		

VA Forecast Information (09/29/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
3.3	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
3.4	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
3.5	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment development utilizing Eclipse is currently based on version 3.3.

General Analysis

Architectural Benefits

- Eclipse provides a flexible and extensible integrated development environment for coding Java Standard Edition and Java Enterprise Edition applications.

Architectural Risks

- Eclipse does not provide all of the tools needed for Java development, requiring end-users to locate, download, and install additional components. This can lead to compatibility issues and a non-functioning environment if not performed carefully.

Tool Type

- Platform
- Framework
- Tool

Tool Usage

- Development

General Assessment

Expected Usage:	Provide developers with an extensible Java-integrated development environment.
Assessment Type:	Refresh
Assessment Date:	11/10/2008
Notes:	Eclipse provides a solid foundation for a Java-integrated development environment, and forms the foundation for the Rational development tools (RSA, RAD) offered by Enterprise Tools Management. The Rational tools should be utilized unless there is a compelling reason to deviate from the standard.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Recommend approval for development teams currently productive with Eclipse. New projects should be using the tool baseline as specified by Enterprise Tools Management.

4.72) Eclipse WTP

General Information

Website:	http://www.eclipse.org/webtools/
Description:	The Eclipse Web Tools Platform (WTP) extends the Eclipse platform with tools for developing Web and Java EE applications. It includes source and graphical editors for a variety of languages, wizards and built-in applications to simplify development, and tools and APIs to support deploying, running, and testing applications.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	Benefits Arch
Decision Process:	TRM v4.1
Decision Date:	10/28/2009

Current Status: Pending Analysis
Introduced By: Benefits ASA
Vendor Name: Eclipse

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	867: Integrated Development Environments (IDE)

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***
- Eclipse - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM

technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.5	6/28/2006		
2.0	6/26/2007		
2.1	12/18/2008		
3.0	6/16/2008		
3.1	6/24/2009		

VA Forecast Information (09/29/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.73) eGate Integrator

General Information

Website: http://developers.sun.com/javacaps/product_list.html#1

Description: eGate Integrator is a J2EE technology-compliant and web-services-

based distributed integration platform. eGate Integrator provides core integration including comprehensive systems connectivity, guaranteed messaging, and robust transformation capabilities. It also provides a unified, single sign-on environment for integration development, deployment, monitoring and management.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: CDCO Supported Architecture Components

Vendor Name: Oracle

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	896: Enterprise Application Integration

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- BusinessWare
- Mirth Connect

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5.1	7/19/2006		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
5.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.74) Encryption Algorithm and IPsec

General Information

Website: http://tools.ietf.org/html/rfc2410

Description: The NULL Encryption Algorithm and Its Use With IPsec defines the NULL encryption algorithm and its use with the IPsec Encapsulating Security Payload (ESP) to provide authentication and integrity without confidentiality.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2410	11/1/1998		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2410	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.75) Encryption Services

General Information

Description: Encryption services use cryptographic algorithms to encode clear text to prevent anyone other than the intended recipient(s) from reading that data. Encryption services are utilized innumerous information protection mechanisms and in infrastructure components required tosupport these mechanisms, such as data at rest encryption, e-mail encryption, and WorldWide Web (WWW) encryption.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
SSL		Servers that use SSL shall be configured to only enable SSL v3.
Data Storage		Data at rest encryption products shall only employ products that use the symmetric data encryption algorithm AES. Other symmetric encryption algorithms require prior approval before use.

Encryption		Adherence to NIST FIPS 140-2 – Security Requirements for Cryptographic Modules is required when using cryptography for Privacy.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
E-mail Encryption	E-mail encryption should be deployed as S/MIME-based solutions. PKI supports trusted digital signatures in S/MIME messages and should be used to implement e-mail encryption.
ISO/IEC 10181-4	Non-repudiation Framework
ISO/IEC 10181-5	Confidentiality Framework

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.76) Enhanced Security Services for S/MIME

General Information

Website: http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

Description: Enhanced Security Services for S/MIME describes four optional security service extensions for S/MIME. The services are:

- signed receipts
- security labels
- secure mailing lists
- signing certificates

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2634	6/1/1999		
RFC 5035	8/1/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2634	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.77) Escrowed Encryption Standard

General Information

Website: http://csrc.nist.gov/publications/PubsFIPS.html

Description: FIPS 185: This standard specifies an encryption/decryption algorithm and a Law Enforcement Access Field (LEAF) creation method which may be implemented in electronic devices and used for protecting government telecommunications when such protection is desired. The algorithm and the LEAF creation method are classified and are referenced, but not specified, in the standard. Electronic devices implementing this standard may be designed into cryptographic modules which are integrated into data security products and systems for use in data security applications. The LEAF is used in a key escrow system that provides for decryption of telecommunications when access to the telecommunications is lawfully authorized.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: NIST

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1	2/9/1994		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.78) Establishing Communication Between Multiple Audiovisual Terminals

General Information

Website:	http://www.itu.int/itu-t/recommendations/index.aspx?ser=H
Description:	ITU-T H.243: Procedures for establishing communication between three or more audiovisual terminals using digital channels up to 1920 kbit/s identifies the system operation for a conference call between three or more audiovisual terminals conforming to ITU-T H.320.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5	10/7/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

5	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.79) European Article Number (EAN-13)

General Information

Website:	http://www.gs1.org/barcodes
Description:	European Article Number (EAN-13) barcode is a barcoding standard which is a superset of the original 12-digit Universal Product Code (UPC) system developed in the United States.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	GS1

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

Forecast Note:	

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.80) Exchange Server

General Information

Website:	http://www.microsoft.com/exchange/
Description:	Exchange Server is the server side of a client-server, collaborative application product. Its major features consist of electronic mail, calendaring, contacts and tasks; support for mobile and web-based access to information; and support for data storage.
Decision:	Approved
Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	Microsoft

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Access Channels	852: Collaboration / Communications

Operating Systems Supported

- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Active Directory - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Secure/Multipurpose Internet Mail Extensions (S/MIME) Message Spec related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2003	9/28/2000		
2007	11/30/2006		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009	CY2010	CY2011

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2003	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.81) Extended Simple Mail Transfer Protocol (ESMTP)

General Information

Website: http://tools.ietf.org/html/rfc1870

Description: Extended Simple Mail Transfer Protocol (ESMTP) defines an extension to the SMTP service whereby an SMTP client and server may interact to give the server an opportunity to decline to accept a message (perhaps temporarily) based on the client's estimate of the message size.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 1870	11/1/1995		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 1870	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.82) eXtensible Access Control Markup Language (XACML)

General Information

Website: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

Description: The eXtensible Access Control Markup Language (XACML) specification defines an XML schema for an extensible access-control policy language.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: OASIS

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Access Control Framework - Standard
- Lightweight Directory Access Protocol (LDAP) - Standard
- Uniform Resource Identifiers (URI) - Standard
- Security Assertion Markup Language (SAML) - Standard
- XML Path Language (XPath) - Standard
- XSL Transformations (XSLT) - Standard
- XML Schema - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	2/18/2003		
1.1	7/24/2003		
2.0	2/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.83) Extensible Authentication Protocol (EAP)

General Information

Website: http://tools.ietf.org/html/rfc5247

Description: Extensible Authentication Protocol (EAP) is an authentication framework which supports multiple authentication methods. EAP typically runs directly over data link layers such as Point-to-Point Protocol (PPP) or IEEE 802, without requiring IP. EAP provides its own support for duplicate elimination and retransmission, but is reliant on lower layer ordering guarantees.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision TRMSP 4.3.2

Process:
Decision Date: 3/14/2008
Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3748	6/1/2004		
RFC 5247	8/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 3748	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.84) Extensible Authentication Protocol Tunneled Transport Layer Security (EAP-TTLS)

General Information

Website: http://tools.ietf.org/html/rfc5281

Description: Extensible Authentication Protocol Tunneled Transport Layer Security (EAP-TTLS) is an EAP (Extensible Authentication Protocol) method that encapsulates a TLS (Transport Layer Security) session, consisting of a handshake phase and a data phase. During the handshake phase, the server is authenticated to the client (or client and server are mutually authenticated) using standard TLS

procedures, and keying material is generated in order to create a cryptographically secure tunnel for information exchange in the subsequent data phase. During the data phase, the client is authenticated to the server (or client and server are mutually authenticated) using an arbitrary authentication mechanism encapsulated within the secure tunnel. The encapsulated authentication mechanism may itself be EAP, or it may be another authentication protocol such as PAP, CHAP, MS-CHAP, or MS-CHAP-V2. Thus, EAP-TTLS allows legacy password-based authentication protocols to be used against existing authentication databases, while protecting the security of these legacy protocols against eaves dropping, man-in-the-middle, and other attacks. The data phase may also be used for additional, arbitrary data exchange.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Transport Layer Security (TLS) Protocol - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 5281	8/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 5281	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.85) Extensible HyperText Markup Language (XHTML)

General Information

Website: http://www.w3.org/TR/

Description: This specification defines XHTML, a reformulation of HTML as an XML application, and three DTDs; Strict, Transitional, and Frameset. These DTDs correspond to the ones defined by HTML. The semantics of the elements and their attributes provide the foundation for future extensibility of XHTML. Compatibility with existing HTML user agents is possible by following a small set of guidelines.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Namespace	XHTML Strict should be used as the preferred namespace.

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	888: Content Rendering

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- HyperText Markup Language (HTML) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	1/26/2000		
1.1	5/31/2001		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010	CY2011	CY2012

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.86) Extensible Markup Language (XML)

General Information

Website: http://www.w3.org/TR/

Description: The Extensible Markup Language (XML) is a subset of SGML that is completely described in the specification. Its goal is to enable generic SGML to be served, received, and processed on the Web in the way that is now possible with HTML. XML has been designed for ease of implementation and for interoperability with both SGML and HTML.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: Benefits Arch

Decision Process: TRM v4.1

Decision Date: 10/28/2009

Current Status: Analysis Completed

Introduced By: Benefits ASA

Vendor Name: W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Federal XML Developer's Guide	This document is an early deliverable of the overall federal strategy for employing XML.
XML Document Structure	XSDs are preferred for describing the structure of XML documents over DTDs.

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	2/10/1998		
1.1	9/29/2006		

VA Forecast Information (10/05/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.0	None	None	None	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
1.1	None	None	None	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. The Benefits Segment use of the XML specification is currently based on version 1.0.

General Analysis

Adoption Benefits

- Openness: A mature, widely adopted industry standard
- Enables the adoption of many other standards that are XML based
- Simplicity - information coded in XML is easy to read and understand

Architectural Benefits

- Internationalization - supports multilingual documents and Unicode
- Interoperability - platform, protocol, and network independent
- Self-description - XML documents contain meta data in the form of tags and attributes
- A common data representation for all levels of the architecture
- Extensibility - new tags can be created as needed
- Facilitates the comparison and aggregation of data

Architectural Risks

- Its expanded size compared with a binary format has an impact on performance

Tier Used

- Client Tier

- Data Tier
- Middle Tier (Integration)
- Middle Tier (Infrastructure)
- Middle Tier (Business)

Tool Usage

- Runtime
- Development

General Assessment

Expected Usage:	XML is a data format standard.
Assessment Type:	Standard
Assessment Date:	11/2/2009
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	XML is a mature, widely adopted industry standard that greatly improves interoperability. It is a core standard upon which many industry standards are based.

4.87) Fault Management

General Information

Description:	Fault management describes the process of preventing, isolating, diagnosing and resolution of problems when they occur. To ensure that critical information is always available at the right place and time, fault management services provide the capability to monitor and detect fault conditions. Fault management can provide the capability for restarting failed processes, and switching over to a secondary device or site, in the event the primary device or site becomes inoperable. A goal of fault management is to ensure COOP and provide rapid network recovery within any defined and agreed upon maximum downtime.
Decision:	Approved

Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Network Management		The network management system shall display management data, monitor and control managed devices, and communicate with management agents. Data link and physical layer parameters shall be monitored by management systems that are based on Management Information Base (MIB) - Remote Monitoring (RMON) standards.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Management Device	A router, server, switch, or end system should be selected on each network to be a local management device.
Problem Notification	Users should be informed about ongoing problems, and given a timeframe for resolution.
Problem Resolution Documentation	After a problem is resolved, the problem/resolution should be tested and then documented in a problem-tracking database.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.88) FDR

General Information

Website:	http://www.fdr.com/products/fdrabr/
Description:	FDR provides standard, high-performance, “non-managed” volume and data set backup and restore services.
Decision:	Approved
Decision Constraints:	This technology’s assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	Innovation

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- z/OS

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- NetBackup

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5.4			

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
5.4	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.89) Fiber Distributed Data Interface (FDDI)

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=16973

Description: ISO/IEC 9314: Fiber Distributed Data Interface (FDDI) provides a 100Mbps optical standard for data transmission in a local area network that can extend in range up to 200 kilometers (124 miles). Although FDDI logical topology is a ring-based token network, it does not use the IEEE 802.5 token ring protocol as its basis; instead, its protocol is derived from the IEEE 802.4 token bus timed token protocol. In addition to covering large geographical areas, FDDI local area networks can support thousands of users. As a standard underlying medium it uses optical fiber, although it can use copper cable, in which case it may be refer to as CDDI. FDDI offers both a Dual-Attached Station (DAS), counter-rotating token ring topology and a Single-Attached Station (SAS), token bus passing ring topology.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Token Ring Physical Layer Protocol (PHY)	This document defines the Physical Layer Protocol (PHY), the upper sublayer of the Physical Layer, for Fibre Distributed Data Interface (FDDI).
Token Ring Media Access Control (MAC)	This document describes the Media Access Control (MAC), the lower sublayer of the Data Link Layer (DLL), for Fibre Distributed Data Interface (FDDI).
Physical Layer Medium Dependent (PMD)	This document defines the structure of the FDDI and specifies the functions and operations necessary to insure interoperability between conforming FDDI implementations.
Single Mode Fibre Physical Layer Medium Dependent (SMF-PMD)	
Hybrid Ring Control (HRC)	
Station Management (SMT)	
Physical layer Protocol (PHY-2)	
Media Access Control-2 (MAC-2)	
Low-cost fibre physical layer medium dependent (LCF-	

PMD)	
Conformance Test Protocol Implementation Conformance Statement (CT-PICS) Proforma	
Abstract test suite for FDDI physical medium dependent conformance testing (FDDI PMD ATS)	

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	Campus Area Network (CAN)*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date

1989			
1990			
1995			
1998			
1999			
2000			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2000	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.90) File Transfer Protocol (FTP)

General Information

Website: http://tools.ietf.org/html/rfc959

Description: File Transfer Protocol (FTP) is a standard network protocol used to exchange and manipulate files over a TCP/IP-based network, such as the Internet. FTP is built on a client-server architecture and utilizes separate control and data connections between the client and server applications. FTP is used with user-based password

authentication or with anonymous user access.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Hypertext Transfer Protocol (HTTP)

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 959	10/1/1985		
RFC 2228	10/1/1997		
RFC 2640	7/1/1999		
RFC 2773	2/1/2000		
RFC 3659	3/1/2007		
RFC 5759	3/1/2010		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 959	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.91) File Transfer Protocol (FTP) Extensions

General Information

Website:	http://tools.ietf.org/html/rfc2428
Description:	File Transfer Protocol (FTP) Extensions for IPv6 and Network Address Translators (NATs) specifies extensions to FTP that will allow the protocol to work over IPv4 and IPv6. In addition, the framework defined can support additional network protocols in the future.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2428	9/1/1998		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2428	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.92) File Transfer Protocol Services

General Information

Description:	File Transfer Protocol (FTP) Services are the portion of a server that listens on a port for FTP requests. The default port is 21.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.93) FileNet P8

General Information

Website: http://www-01.ibm.com/software/data/content-management/filenet-p8-platform/

Description: FileNet P8 is a unified platform for enterprise content management (ECM). The core of the platform is provided by:
- FileNet Content Manager
- FileNet Business Process Manager
- FileNet Records Manager

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: Benefits Arch

Decision Process: TRM v4.1

Decision Date: 10/28/2009

Current Status: Pending Analysis

Introduced By: Benefits ASA

Vendor Name: IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	895: Middleware

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***
- Active Directory - ***(required libraries)***
- WebLogic Server - ***(required libraries)***
- Oracle Database - ***(required libraries)***
- Internet Explorer - ***(required for some configurations)***
- Firefox - ***(required for some configurations)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.5	12/21/2005	4/30/2009	9/30/2010
4.0	3/15/2007		4/30/2011
4.5	12/12/2008		

VA Forecast Information (09/29/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or

production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
4.5	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.94) Fire Walling

General Information

Description: A firewall is a system designed to prevent unauthorized access to or from a different parts of a network architecture. In addition to providing network access control, a properly configured and managed firewall can provide network intrusion prevention and limit damage caused by any single intrusion or security event.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
VA Firewall Policy	VA Memorandum Aug 29, 2001	Attachment to the VA Assistant Secretary for Information Technology Memorandum of August 29, 2001 “Securing the Department’s Information Technology Infrastructure”

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Layer Gateway Network Firewalls	All information systems should use application layer gateway network firewalls to secure connections to public networks. Network firewalls can be centrally located, centrally managed,and shared between multiple sites only if a secure intranet is used to connect the sites.
Default Restrictive Policy	Network firewalls should be configured with the most restrictive security policy possible, “thatwhich is not expressly allowed is denied.”
Network Firewalls Compatibility	Information systems should ensure that any protocols used across public inter-networks arecompatible with application layer gateway network firewalls.
Host-based Firewalls	Host-based firewalls should be used on: Large web portals or web farms, servers that provide critical services, i.e., database servers, e-mail servers, etc., and services that process and store critical or proprietary information, i.e., payroll,accounting, human resources, etc.
Personal Firewalls	Personal firewalls should be used on all client workstations. Personal firewalls on client workstations should be centrally managed.
NIST SP 800-41	Guidelines on Firewalls and Firewall Policy

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.95) Firefox

General Information

Website:	http://www.mozilla.com/en-US/
Description:	Firefox is a widely utilized Web browser. It provides access to HeV thin client applications and serves as the operating environment for Web based client side components.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	TRM Team
Vendor Name:	Mozilla

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Access Channels	850: Web Browser

Operating Systems Supported

- Red Hat Linux
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required for some configurations)***
- XSL Transformations (XSLT) - ***(required for some configurations)***

Comparable Technologies/Standards:

- Internet Explorer

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.5	11/29/2005	5/30/2007	
2.0	10/24/2006	12/18/2008	4/30/2009
3.0	6/17/2008		
3.5	6/30/2009		

VA Forecast Information (10/06/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009	CY2010	CY2011

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2.0	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
3.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
3.5	None	None	Evaluation	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. The Benefits Segment use of Firefox is currently based on version 1.5.

General Analysis

Architectural Benefits

- As a modular, standards-based Web browser, Firefox will enable the scalable and flexible deployment of thin-client applications.

Architectural Risks

- The introduction of more than one Web browser (to coexist with Internet Explorer) creates multiple versions of the JavaScript interpreter, application add-ins (plug-ins), and could result in compatibility issues for HeV developers.

EA Requirement

- ENTR 955 (Inactive) - Web browser based applications shall not require or encourage users to choose any specific browser or viewer software.

Tool Usage

- Firefox is collaborating with the Web Standards Project to identify and improve compliance with industry standards. Additional information can be found at: http://developer.mozilla.org/en/docs/Web_Standards.

General Assessment

Expected Usage:	Firefox provides a standardized deployment and operational platform at the client level in the HeV architecture.
Assessment Type:	Refresh
Assessment Date:	9/16/2008
Notes:	
Recommendati	Approve

on:	
Recommendation Constraints:	
Recommendation Justification:	Recommend approval as an alternative Web browser.

4.96) Frame Structure in Audiovisual Teleservices

General Information

Website:	http://www.itu.int/itu-t/recommendations/index.aspx?ser=H
Description:	ITU-T H.221: Frame Structure for a 64 to 1920 kbit/s Channel in Audiovisual Teleservices defines a frame structure for audiovisual teleservices in single or multiple B or H0 channels or a single H11 or H12 channel which makes the best use of the characteristics and properties of the audio and video encoding algorithms, of the transmission frame structure and of the existing Recommendations.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
7	3/15/2004		
7.1	9/13/2005		
8	3/16/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010	CY2011	CY2012

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
7.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.97) Frame-synchronous Control and Indication Signals for Audiovisual Systems

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=H

Description: ITU-T H.230: Frame-synchronous Control and Indication Signals for Audiovisual Systems details the Control and Indication (C&I) related to video and audio; means of transmitting numbers and characters; C&I for maintenance purposes; for simple multipoint conferences not using protocol in the Meridian Lossless Packing (MLP) channel; for channel aggregation; and for the transfer of network addresses.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
6	3/15/2004		
6.1	10/7/2005		
7	3/16/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on

the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
6.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.98) General Parallel File System (GPFS)

General Information

Website: http://www-03.ibm.com/systems/software/gpfs/index.html

Description: The General Parallel File System (GPFS) is a high-performance shared-disk clustered file system. GPFS provides online storage management, scalable access, and integrated information lifecycle management tools capable of managing petabytes of data and billions of files.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: CDCO Supported Architecture Components

Vendor Name: IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Business Logic	890: Platform Independent Technologies

Operating Systems Supported

- AIX
- Red Hat Linux
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date

2.3	5/1/2008		
3.1	7/1/2009		
3.2	9/1/2007		
3.3	9/1/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2.3	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.99) Graphics Interchange Format (GIF)

General Information

Website: http://www.w3.org/Graphics/GIF/spec-gif89a.txt

Description: The Graphics Interchange Format defines a protocol intended for the on-line transmission and interchange of raster graphic data in a way that is independent of the hardware used in their creation or display.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision EA

Source:	
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	888: Content Rendering

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1990	7/31/1990		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.100) Health Information Data Exchange

General Information

Description: Health Information Data Exchange standards support batch-oriented, messaging capability (i.e., orders, results,admission, discharge, transfer, etc.) between health information systems.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Application Exchange	HL7 messages should be used when the application is hosted on a PC or Server-based platform, not a micro-controller platform.
Device Exchange	The FDA has not accepted HL7 for use in regulated medical devices.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.101) HyperText Markup Language (HTML)

General Information

Website: http://www.w3.org/TR/

Description:	HyperText Markup Language (HTML) is the predominant markup language for web pages. It provides a means to create structured documents by denoting structural semantics for text such as headings, paragraphs, lists etc as well as for links, quotes, and other items. It allows images and objects to be embedded and can be used to create interactive forms.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Styles	External Cascading Style Sheets (CSS) are the preferred method for formatting HTML, followed by embedded CSSs, and lastly by embedded HTML

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	886: Static Display

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Cascading Style Sheets (CSS) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.2	1/14/1997		
4.0	12/24/1999		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
4.0	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.102) Hypertext Transfer Protocol (HTTP)

General Information

Website:	http://tools.ietf.org/html/rfc2817
Description:	The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. It is a generic, stateless, protocol which can be used for many tasks beyond its use for hypertext, such as name servers and distributed object management systems, through extension of its request methods, error codes and headers. A feature of HTTP is the typing and negotiation of data representation, allowing systems to be built independently of the data being transferred.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description

HTTP Over TLS	This document describes how to use TLS to secure HTTP connections over the Internet.
Upgrading to TLS Within HTTP/1.1	This document explains how to use the Upgrade mechanism in HTTP/1.1 to initiate Transport Layer Security (TLS) over an existing TCP connection.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- File Transfer Protocol (FTP)

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.1	6/1/1999		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is

considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.103) Hypertext Transfer Protocol Services

General Information

Description: Web servers are World Wide Web platforms for creating, managing, and intelligibly distributing informationand on-line applications. The web server should address Internet message handling, advanced authoring,and a range of security issues. Most web servers enable users to navigate, create, edit, and publish HTML documents in a user-friendly environment. Web servers and application servers allow developers to create arbitrarily complex and highly scalable n-tier applications that can support rapidly growing e-Business needs. They provide Web connectivity, e-Business functionality, runtime services-e.g., load balancing, failover, hot swapping, transaction management, object management, session management, connection pooling - component integration, and application and data integration services.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.104) Identification Authentication

General Information

Description: Identification & Authentication is a set of security measures designed to establish the validity of an identity of a user, user device, or other entity.

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. Currently, authentication is most commonly done through the use of logon passwords. Some business processes may require a more stringent

authentication process. The use of digital certificates issued and verified by a Certificate Authority (CA) as part of a Public Key Infrastructure (PKI) is another way to perform authentication with higher assurance. Logically, authentication precedes authorization.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Password Management Policy		VA Information System Account and Password Management Policy (January 2000)
Protection Profiles		VA Security Standards Profile Summary and Department of Veterans Affairs Protection Profiles for Information Systems (November 13, 2001)
Authentication Methods		Authentication methods and technologies implemented by the VA shall offerno less than two-factor authentication.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
NSA - Network Security Guide	The 60 Minute Network Security Guide
NIST FIPS 48	Guidelines On Evaluation Of Techniques For Automated Personal Identification
NIST FIPS 190	Guideline For The Use Of Advanced Authentication Technology Alternatives
NIST SP 800-12	An Introduction to Computer Security: The NIST Handbook

NIST SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
NIST SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
IETF RFC 2989	Criteria for Evaluating AAA Protocols for Network
IETF RFC 3127	Authentication, Authorization, and Accounting: Protocol Evaluation
IETF RFC 3549	Authentication, Authorization and Accounting (AAA) Transport Profile
ISO/IEC 10181-2	Authentication Framework
ASTM E1985	Guide for User Authentication and Authorization
ASTM E1714	Standard Guide for Properties of a Universal Healthcare Identifier (UHID)

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.105) Identification Cards - Integrated Circuit(s) Cards With Contacts

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=29257

Description: ISO/IEC 7816: Identification Cards - Integrated Circuit(s) Cards With

	Contacts is a standard related to electronic identification cards with contacts, especially smart cards.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Physical characteristics	
Organization, security and commands for interchange	
Interindustry commands for Structured Card Query Language (SCQL)	
Commands for security operations	This document specifies interindustry commands for integrated circuit cards (either with contacts or without contacts) that may be used for ryptographic operations.
Commands for card management	This document specifies interindustry commands for integrated circuit cards (both with contacts and without contacts) for card and file management.

Electronic signals and answer to reset for synchronous cards	This document specifies the power, signal structures, and the structure for the answer to reset between an integrated circuit card(s) with synchronous transmission and an interface device such as a terminal.
Personal verification through biometric methods	This document specifies the usage of interindustry commands and data objects related to personal verification through biometric methods in integrated circuit cards.
Cards with contacts -- USB electrical interface and operating procedures	Tihs document specifies the operating conditions of an integrated circuit card that provides a USB interface. An integrated circuit card with a USB interface is named USB-ICC.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date

1998			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1998	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.106) Internet Control Message Protocol (ICMP)

General Information

Website: http://tools.ietf.org/html/rfc792

Description: The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol Suite. It is chiefly used by networked computers' operating systems to send error messages - indicating, for instance, that a requested service is not available or that a host or router could not be reached.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 792	9/1/1981		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 792	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.107) Internet Explorer

General Information

Website: http://www.microsoft.com/windows/internet-explorer/welcome.aspx

Description: Internet Explorer is the standard Web browser for HeV (reference VA Directive 6401). Internet Explorer provides access to HeV thin-client applications and Internet-VA intranet sites-applications.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision ARB

Source:	
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	TRM Team
Vendor Name:	Microsoft

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Access Channels	850: Web Browser

Operating Systems Supported

- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required for some configurations)***
- XSL Transformations (XSLT) - ***(required for some configurations)***

Comparable Technologies/Standards:

- Firefox

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM

technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
6.0	8/30/2002	10/1/2006	8/1/2012
7.0	10/1/2006	10/2/2011	10/1/2016
8.0	3/19/2009		

VA Forecast Information (10/16/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
6.0	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
7.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	Field Office IE7 Memo The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment development and deployment using IE is currently based on version 6.

General Analysis

Architectural Area

- Application

Architectural Benefits

- Using a modular browser enables the deployment HeV thin-client applications.

Architectural Risks

- Security issues: as the Web browser market-share leader, Internet Explorer is an attractive target for criminals to exploit security flaws.

EA Requirement

- ENTR 952: VHA shall comply with standards as specified in the VA TRM/SP

Tier Used

- Client Tier
- Presentation Tier (Web)

Tool Type

- Tool

Tool Usage

- Runtime

General Assessment

Expected Usage:	Internet Explorer (IE) provides a standardized deployment and operational platform at the client level in the HeV architecture.
Assessment Type:	Refresh
Assessment Date:	10/2/2008
Notes:	IE 7 had an atypically lengthy development cycle as a result of litigation disputes and extensive product testing. The release of IE 8 is imminent, although no release date has been specified.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Recommend approval as Internet Explorer is successfully implemented in the HeV infrastructure.

4.108) Internet Key Exchange (IKE)

General Information

Website:	http://www.rfc-editor.org/rfcsearch.html
Description:	The Internet Key Exchange (IKE) is a protocol using part of Oakley and part of Secure Key Exchange Mechnanism (SKEME) in

conjunction with Internet Security Association and Key Management Protocol (ISAKMP) to obtain authenticated keying material for use with ISAKMP, and for other security associations such as Authentication Header (AH) and Encapulating Security Payload (ESP) for the IETF IPsec Domain of Interpretation (DOI).

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0 (RFC 2409)	11/1/1998		
2.0 (RFC 4306)	12/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.0 (RFC 2409)	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.109) Internet Message Access Protocol (IMAP)

General Information

Website: http://tools.ietf.org/html/rfc1734

Description: Internet Message Access Protocol (IMAP) describes the optional AUTH command, for indicating an authentication mechanism to the server, performing an authentication protocol exchange, and optionally negotiating a protection mechanism for subsequent protocol interactions.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 1734	12/1/1994		
RFC 1939	5/1/1996		
RFC 2449	11/1/1998		
RFC 5034	7/1/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2449	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.110) Internet Message Format

General Information

Website:	http://tools.ietf.org/html/rfc2822
Description:	Internet Message Format specifies a syntax for text messages that are sent between computer users, within the framework of "electronic mail" messages.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	871: Web Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2822	4/1/2001		
RFC 4021	3/1/2005		
RFC 5322	10/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 4021	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.111) Internet Protocol (IP)

General Information

Website:	http://tools.ietf.org/html/rfc791
Description:	Internet Protocol (IP) provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses. The internet protocol also provides for fragmentation and reassembly of long datagrams, if necessary, for transmission through "small packet" networks.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 791	9/1/1981		
RFC 1349	7/1/1992		
RFC 2474	12/1/1998		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010	CY2011	CY2012

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 791	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.112) Internet Protocol Version 6 (IPv6)

General Information

Website: http://tools.ietf.org/html/rfc2460

Description: Internet Protocol Version 6 (IPv6) Specification is an Internet Layer protocol for packet-switched internetworks. IPv6 is the next-generation Internet Protocol version designated as the successor to IPv4.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2460	12/1/1998		
RFC 5095	12/1/2007		
RFC 5722	12/1/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is

considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2460	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.113) Internet Web

General Information

Description: The Internet is a worldwide system of computer networks in which users at any onecomputer can, if they have permission, get information from any other computer.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Internet/Intranet	VA Directive	This directive defines the organizational

Services	6102	responsibilities for all Web activities that govern and/or are related to posting, editing, maintaining, and removing files to or from the Internet and Intranet, the use of emerging Web-based technologies and new uses of existing approved technologies.
Internet/Intranet Services	VA Handbook 6102	This Handbook provides procedures relating to the establishment and administration of a VA Internet and/or Intranet site, and/or site operating on behalf of VA, and/or related service; it also provides procedures for publishing VA information on the World Wide Web (www).

Guidelines and Best Practices

No guidelines have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Delivery Channels	854: Internet

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.114) Intranet Web

General Information

Description: An Intranet is a private network that is contained within an enterprise. It may consist of many interlinked local area networks and is used to share company information and resources among

employees.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Internet/Intranet Services	VA Directive 6102	This directive defines the organizational responsibilities for all Web activities that govern and/or are related to posting, editing, maintaining, and removing files to or from the Internet and Intranet, the use of emerging Web-based technologies and new uses of existing approved technologies.
Internet/Intranet Services	VA Handbook 6102	This Handbook provides procedures relating to the establishment and administration of a VA Internet and/or Intranet site, and/or site operating on behalf of VA, and/or related service; it also provides procedures for publishing VA information on the World Wide Web (www).

Guidelines and Best Practices

No guidelines have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Delivery Channels	855: Intranet

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.115) Intrusion Detection and Prevention Systems (IDPS)

General Information

Website:	http://csrc.nist.gov/publications/PubsSPs.html
Description:	Intrusion Detection Prevention Systems (IDPS) describes the characteristics of IDPS technologies and provides recommendations for designing, implementing, configuring, securing, monitoring, and maintaining them. The types of IDPS technologies are differentiated primarily by the types of events that they monitor and the ways in which they are deployed.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	NIST

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Security Controls*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
SP 800-31	11/1/2001		2/1/2007
SP 800-94	2/1/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
SP 800-31	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.116) Intrusion Detection Devices

General Information

Description: Intrusion detection services monitor the events occurring in a computer system or network and analyze them for signs of intrusion. An Intrusion Detection System (IDS) is a software or hardware system that automates the process of monitoring the events occurring in a computer system or network, and then analyzing these events forsigns of security problems. Host-Based Intrusion Detection Systems (HIDS) services monitor specific files, logs and registry settings on asingle machine (workstation or server) and can alert on any access, modification, deletion, and copying of the monitored object. The role of a HIDS is to flag any tampering with a specific machine and automatically replace altered files when changed to ensure data integrity. Network-based Intrusion Detection Systems, (NIDS) provide the ability to monitor different segments of the network in order to discover, define and warn about attacks to the network infrastructure.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision TRMSP 4.3.2

Process:
Decision Date: 3/14/2008
Current Status: Analysis Completed
Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Placement of IDS	The IDS are not the first line of defense. If firewalls and filtering routers are already in place, thenIDS sensors should be placed inside the network to test the effectiveness of firewall and router policies. Placing sensors inside and outside the firewall provides a pre-emptive capability inidentifying the threat in the early stages of reconnaissance (i.e., scanning and probing).
Use multiple products	Whenever possible, IDS deployments should combine products from more than one vendor and more than one type. This gives added assurance that attacks can be detected, since not all the sensors types may be able to detect all the known attacks in any given environment or operating condition.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Security Controls*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.117) IP Authentication Header (AH)

General Information

Website:	http://www.rfc-editor.org/cgi-bin/rfcsearch.pl
Description:	The IP Authentication Header (AH) is used to provide connectionless integrity and data origin authentication for IP datagrams and to provide protection against replays.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Internet Protocol (IP) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2402	11/1/1998		
RFC 4302	12/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 4302	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.118) IP Encapsulating Security Payload (ESP)

General Information

Website: http://www.rfc-editor.org/rfcsearch.html

Description: Encapsulating Security Payload (ESP) protocol is designed to provide a mix of security services in IPv4 and IPv6. ESP is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic flow confidentiality.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Internet Protocol (IP) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 4303	12/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 4303	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.119) IP Network Address Translator (NAT)

General Information

Website:	http://tools.ietf.org/html/rfc2663
Description:	Network Address Translation (NAT) is a method by which IP addresses are mapped from one realm to another, in an attempt to provide transparent routing to hosts. Traditionally, NAT devices are used to connect an isolated address realm with private unregistered addresses to an external realm with globally unique registered addresses. This document attempts to describe the operation of NAT devices and the associated considerations in general, and to define the terminology used to identify various flavors of NAT.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IP Routing Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Internet Protocol (IP) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2663	8/1/1999		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010	CY2011	CY2012

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2663	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.120) IP Routing Services

General Information

Description: IP routing services enable packet flow from network to network through routers. The path that a router uses to deliver a packet is defined in its routing table. Routers can statically or dynamically learn the location of traffic destinations from routing protocols. Dynamic routing allows routers to share routing information automatically. If a destination route changes, neighboring routers are informed of the change. The method the router takes to determine a route is described in the specifications of the routing protocol. The routing protocol attempts to find the best path between any source and destination pair in the network. IP routing services provide the capability for routers to find optimum routes, and alternate routes, in the case of network failure or congestion.

Network Address Translation (NAT) performs transparent routing services by performing IP address translation. Transparent routing services are defined as the forwarding of packets from one network to another, and do not require the exchange of routing information. IP address translation is needed when a network's internal IP addresses cannot be used outside the network either because they are private and not valid for use outside, or because the internal addressing must be kept private from the external network. NAT provides the capability to translate public and private addresses in both directions of traffic.

Decision: Approved

Decision The Routing Information Protocol (RIP) is not approved for use.

Constraints:

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Campus IGP	Campus Interior Gateway Protocols (IGPs) may run another IGP, such as OSPF, within its own campus LAN environment. For design consistency and scalability, it is recommended that the IGP on the LAN be the same as the region WANs.
IP Routing Path	To determine an IP routing path to a remote device, use a middleware operating system utility. The utility may bereferred to as traceroute or tracert, depending on the operating system in use.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.121) IPsec Transport Mode for Dynamic Routing

General Information

Website:	http://tools.ietf.org/html/rfc3884
Description:	IPsec can secure the links of a multihop network to protect communication between trusted components, e.g., for a secure virtual network (VN), overlay, or virtual private network (VPN). Virtual links established by IPsec tunnel mode can conflict with routing and forwarding inside VNs because IP routing depends on references to interfaces and next-hop IP addresses. The IPsec tunnel mode specification is ambiguous on this issue, so even compliant implementations cannot be trusted to avoid conflicts. An alternative to tunnel mode uses non-IPsec IPIP encapsulation together with IPsec transport mode, which we call IIPtran. IPIP encapsulation occurs as a separate initial step, as the result of a forwarding lookup of the VN packet. IPsec transport mode processes the resulting (tunneled) IP packet with an SA determined through a security association database (SAD) match on the tunnel header. IIPtran supports dynamic routing inside the VN without changes to the current IPsec architecture. IIPtran demonstrates how to configure any compliant IPsec implementation to avoid the aforementioned conflicts. IIPtran is also compared to several alternative mechanisms for VN routing and their respective impact on IPsec, routing, policy enforcement, and interactions with the Internet Key Exchange (IKE).
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Internet Protocol (IP) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3884	9/1/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be

supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 3884	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.122) IPsec-Network Address Translation (NAT)

General Information

Website: http://tools.ietf.org/html/rfc3715

Description: IPsec-Network Address Translation (NAT) Compatibility Requirements describe known incompatibilities between Network Address Translation (NAT) and IPsec, and describe the requirements for addressing them.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Internet Protocol (IP) - Standard
- Network Address Translation - Protocol Translation (NAT-PT) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3715	3/1/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the

responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 3715	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.123) IPv6 Client Services

General Information

Description:

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
MPLS	The current process for VPNs with IPv6 is to tunnel over an MPLS IPv4 backbone. Currently there is no ability to establish an MPLS IPv6 backbone. There is the ability to Overlap IPv6 VPNs through VRF.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.124) IPv6 over Point-to-Point Protocol (PPP)

General Information

Website: http://tools.ietf.org/html/rfc2472

Description: IP Version 6 (IPv6) over Point-to-Point Protocol (PPP) defines the method for transmission of IP Version 6 packets over PPP links as well as the Network Control Protocol (NCP) for establishing and configuring the IPv6 over PPP. It also specifies the method of forming IPv6 link-local addresses on PPP links.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision FA

Source:	
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Internet Protocol (IP) - Standard
- Point-to-Point Protocol (PPP) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2472	12/1/1998	9/1/2007	
RFC 5072	9/1/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2472	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.125) IPv6 Performance

General Information

Description: IPv6 performance test should be considered as a first step in creating a baseline, not only for all future IPv6 testing but also to understand any performance differences that may exist in any device that forwards IPv4 and/or IPv6 traffic. These performance tests should not be limited to Quality of Service (QoS), but should also include Quality of Experience(QoE), to show clear delineation between what is happening on the network, and what the end-user

	is experiencing.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.126) IPv6 Prefix Options for Dynamic Host Configuration

Protocol (DHCPv6)

General Information

Website: http://tools.ietf.org/html/rfc3633

Description: The Prefix Delegation options provide a mechanism for automated delegation of IPv6 prefixes using the Dynamic Host Configuration Protocol (DHCP). This mechanism is intended for delegating a long-lived prefix from a delegating router to a requesting router, across an administrative boundary, where the delegating router does not require knowledge about the topology of the links in the network to which the prefixes will be assigned.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Internet Protocol (IP) - Standard
- Dynamic Host Configuration Protocol (DHCP) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3633	12/1/2003		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 3633	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.127) IPv6/IPv4 Dual Stack Internet Access Service Model

General Information

Website:	http://tools.ietf.org/html/rfc4241
Description:	IPv6/IPv4 Dual Stack Internet Access Service Model is a digest of the user network interface specification of NTT Communications' dual stack ADSL access service, which provide a IPv6/IPv4 dual stack services to home users. In order to simplify user setup, these services have a mechanism to configure IPv6 specific parameters automatically. The model focuses on two basic parameters: the prefix assigned to the user and the addresses of IPv6 DNS servers, and it specifies a way to deliver these parameters to Customer Premises Equipment (CPE) automatically.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Internet Protocol (IP) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 4241	12/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

RFC 4241	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.128) Java Data Objects (JDO)

General Information

Website:	http://java.sun.com/jdo/
Description:	The JDO specification provides for interface-based definitions of data stores and transactions; and selection and transformation of persistent storage data into native Java programming language objects.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	Sun Microsystems

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Management	893: Database Connectivity

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Java SE

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	4/30/2002		
2.0	5/1/2006		
2.1	3/17/2008		
2.2	10/24/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2.1	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
2.2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.129) Java EE

General Information

Website: http://java.sun.com/javaee/index.jsp

Description: The Java Platform, Enterprise Edition, or Java EE (formerly known as J2EE) is a platform for large scale server programming in the Java programming language. Java EE differs from the Standard Edition (SE) of Java in that it adds additional libraries that provide functionality to deploy fault-tolerant, distributed, multi-tier Java software, based largely on modular components running on an application server. It is also a reference implementation of the Java EE specification.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: ARB

Decision Process: TRM v2

Decision Date: 9/17/2008

Current Status: Analysis Completed

Introduced By: Extended Tool List (ETL)

Vendor Name: Sun Microsystems

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Data Types	Char Type, Unsigned Numerical Types, and Enumerations data types should always be avoided because they are not completelydefined in the JAX-RPC and/or XML Schema specification and can lead to unpredictable results. Alternatively, arrays can be used instead of enumerated collections. Complex Data types & Binary Data (via SOAP attachments) should be avoided when JAX-RPC is used to communicate with web services implemented in other languages. Alternatively, binary data can be mapped to xsd:base64Binary and xsd:hexBinary, but this mapping can be inefficient with large amounts of data.

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Java Platform, Enterprise Edition 5 Specification (Java EE 5)	
Implementing Enterprise Web Services	This specification defines the programming model and runtime architecture for implementing web services in Java.
Java API for XML-Based Web Services (JAX-WS)	Added in Java EE 5, JAX-WS is a fundamental technology for developing SOAP based and RESTful Java Web services. JAX-WS is designed to take the place of JAX-RPC in Web services and Web applications.
Java API for XML-Based RPC (JAX-RPC)	Java APIs to support emerging industry XML based RPC standards.
Java Architecture for XML Binding (JAXB)	JAXB provides a convenient way to process XML content using Java objects by binding its XML schema to Java representation.
SOAP with	The SOAP with Attachments API for Java (SAAJ) provides the API for

Attachments API for Java (SAAJ)	creating and sending SOAP messages by means of the javax.xml.soap package. It is used for the SOAP messaging that goes on behind the scenes in JAX-RPC and JAXR implementations.
Streaming API for XML (StAX) - Added in Java EE 5	The Streaming API for XML (StAX) is a Java based API for pull-parsing XML. StAX provides an alternative to SAX, DOM, TrAX, and DOM for developers looking to do high-performance stream filtering, processing, and modification, particularly with low memory and limited extensibility requirements.
Web Service Metadata for the Java Platform	Added in Java EE 5, Web Services Metadata defines an annotated Java format that that uses JavaTM Language Metadata (JSR 175) to enable easy definition of Java Web Services in a J2EE container.
Java Servlet	The Java Servlet specification.
JavaServer Faces - Added in Java EE 5	
JavaServer Pages (JSP)	The JavaServer Pages (JSP) specification.
JavaServer Pages Standard Tag Library (JSTL)	Added in Java EE 5, JSTL is a standard tag library for JSP pages.
Enterprise JavaBeans	The Enterprise JavaBeans specification extends the architecture with integration with JMS, improved support for entity bean persistence, a portable query language for finder methods, support for server interoperability, support for web services, extensions to message-driven beans, enhancements to EJB QL, and a container-managed timer service.
J2EE Connector Architecture (JCA)	The J2EE Connector architecture defines a standard architecture for integrating Java applications with existing back-end Enterprise Information systems.
Common Annotations for the Java Platform	This specification provides annotations for common semantic concepts in the J2SE and J2EE platforms that apply across a variety of individual technologies.
Java Message Service API (JMS)	
Java Persistence API (JPA) - Added in Java EE 5	he Java Persistence API is the Java API for the management of persistence and object/relational mapping for Java EE and Java SE environments.
Java Transaction API (JTA)	Java Transaction API (JTA) specifies standard Java interfaces between a transaction manager and the parties involved in a distributed transaction system: the resource manager, the application server, and the transactional applications.

JavaBeans Activation Framework (JAF)	The JavaBeans Activation Framework specification is a data typing and registry technology that is a Standard Extension to the Java Platform.
JavaMail	The JavaMail API provides a platform-independent and protocol-independent framework to build mail and messaging applications.
J2EE Application Deployment	The J2EE Application Deployment specification provides a complete description of the APIs required by the J2EE platform to enable development of platform-independent deployment tools.
J2EE Management	The Java 2 Platform, Enterprise Edition Management Specification will provide server vendors and tool vendors with a standard model for managing the J2EE Platform.
Java Authorization Contract for Containers	This document defines a contract between containers and authorization service providers that will result in the implementation of providers for use by containers
Java Platform 2, Enterprise Edition Specification (J2EE 1.4)	
Java API for XML Parsing (JAXP)	The Java API for XML Parsing (JAXP) allows developers to easily use XML Parsers in their applications via the industry standard SAX and DOM APIs.
Java API for XML Processing	The Java API for XML Processing defines a set of implementation independent portable APIs supporting XML Processing.
Java API for XML Messaging (JAXM)	JAXM provides an API for packaging and transporting business transactions using on-the-wire protocols being defined by ebXML.org, Oasis, W3C and IETF.
Java API for XML Registries (JAXR)	JAXR provides an API for a set of distributed Registry Services that enables business-to-business integration between business enterprises, using the protocols being defined by ebXML.org, Oasis, ISO 11179.
JDBC API	The JDBC API is the industry standard for database-independent connectivity between the Java programming language and a wide range of databases. The JDBC API provides a call-level API for SQL-based database access. JDBC technology allows you to use the Java programming language to exploit "Write Once, Run Anywhere" capabilities for applications that require access to enterprise data.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	887: Dynamic Server-Side Display
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- WebLogic Server - ***(required for some configurations)***

Comparable Technologies/Standards:

- Java SE

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5.0 (aka 1.5)	4/28/2006		
5.2	12/15/2006		
5.3	5/7/2007		
5.4	2/11/2008		
5.5	6/18/2008		

VA Forecast Information (10/14/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**

5.2	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
5.3	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
5.4	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
5.5	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment java development is currently based on Java EE version 5.0.

General Analysis

Architectural Area

- Application
- Data
- Integration

Architectural Benefits

- Java EE provides a standardized, object oriented, application programming language to realize the components of the modular SOA architecture in a platform independent manner.

Architectural Risks

- Performance - applying Java EE to achieve high performance requires both significant programming skill and environmental tuning.
- Complexity - Java EE implementations can achieve excessive numbers of components and resulting system complexities
- Troubleshooting - a Java EE implementation can be designed to leverage capabilities provided by other enterprise components. This can lead to multi-disciplinary troubleshooting of enterprise issues.

Tier Used

- Middle Tier (Infrastructure)
- Client Tier
- Data Tier
- Presentation Tier (Web)
- Middle Tier (Business)
- Middle Tier (Integration)

Tool Type

- Framework

Tool Usage

- Development
- Runtime

General Assessment

Expected Usage:	Java EE is used to create the services, operational, and business logic components of the HeV architecture.
Assessment Type:	Standard
Assessment Date:	9/24/2008
Notes:	Java EE is a Java implementation and a standard, so the technology can be used to deploy functionality and to evaluate Java-based technologies.
Recommendation:	N/A
Recommendation Constraints:	
Recommendation Justification:	

4.130) Java SE

General Information

Website:	http://java.sun.com/javase/index.jsp
Description:	Java Standard Edition (previously known as Java 2 Standard Edition) is the specifications of a java virtual machine and java API (Application Programming Interface). It has been developed under the Java Community Process. JSR 59 was the umbrella specification for J2SE 1.4 and JSR 176 specified J2SE 5.0 (Tiger). Java SE 6 (Mustang) was released under JSR 270. The Java Platform API specification includes: • **User interface Toolkits:** AWT, Swing, Java 2D, Accessibility, Drag n Drop, Input Methods, Image I/O, Print Service, Sound • **Integration Libraries:** IDL, JBDC, JNDI, RMI, RMI-IIOP, Scripting

- **Other Base Libraries:** Beans, Intl Support, I/O, JMX, JNI, Math, Networking, Override Mechanism, Security, Serialization, Extension Mechanism, XML JAXP
- **lang and util Base Libraries:** lang and util, Collections, Concurrency Utilities, JAR, Logging, Management, Preferences API, Ref Objects, Reflection, Regular Expressions, Versioning, Zip, Instrument

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: ARB

Decision Process: TRM v2

Decision Date: 9/17/2008

Current Status: Analysis Completed

Introduced By: Extended Tool List (ETL)

Vendor Name: Sun Microsystems

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Java Language	
Java Virtual Machine	
Java Compiler API	A service provider API that allows a Java program to select and invoke a Java Language Compiler programmatically.
Java Platform, Standard Edition 1.4 (J2SE 1.4)	The Java SE 1.4 specification defines a wide range of general purpose APIs and also includes the Java Language Specification and the Java Virtual Machine Specification. In addition to being used standalone on servers, Java SE is also used as the base for Java Platform, Enterprise Edition ("Java EE").
Java Platform, Standard Edition	The Java SE 5.0 specification defines a wide range of general purpose APIs and also includes the Java Language Specification and the Java

5 (Java SE 5)	Virtual Machine Specification. In addition to being used standalone on servers, Java SE is also used as the base for Java Platform, Enterprise Edition ("Java EE").
Java Platform, Standard Edition 6 (Java SE 6)	The Java SE 6.0 specification defines a wide range of general purpose APIs and also includes the Java Language Specification and the Java Virtual Machine Specification. In addition to being used standalone on servers, Java SE is also used as the base for Java Platform, Enterprise Edition ("Java EE").
Java API for XML Processing (JAXP)	JAXP defines a set of implementation independent portable APIs supporting XML Processing.
JDBC API	The JDBC API is the industry standard for database-independent connectivity between the Java programming language and a wide range of databases. The JDBC API provides a call-level API for SQL-based database access. JDBC technology allows you to use the Java programming language to exploit "Write Once, Run Anywhere" capabilities for applications that require access to enterprise data.
Java Business Integration (JBI)	This specification extends J2EE and J2SE with business integration SPIs.
Java API for XML-Based Web Services (JAX-WS)	JAX-WS is a fundamental technology for developing SOAP based and RESTful Java Web services. JAX-WS is designed to take the place of JAX-RPC in Web services and Web applications.
Java Architecture for XML Binding (JAXB)	JAXB provides a convenient way to process XML content using Java objects by binding its XML schema to Java representation.
Streaming API for XML (StAX)	Added in Java SE 6, the Streaming API for XML (StAX) is a Java based API for pull-parsing XML. StAX provides an alternative to SAX, DOM, TrAX, and DOM for developers looking to do high-performance stream filtering, processing, and modification, particularly with low memory and limited extensibility requirements.
Web Services Metadata for the Java Platform	This specification defines an annotated Java format that that uses JavaTM Language Metadata (JSR 175) to enable easy definition of Java Web Services in a J2EE container.
XML Digital Signature APIs	This document defines and incorporates a standard set of high-level implementation-independent APIs for XML digital signatures services. The XML Digital Signature specification is defined by the W3C.
Common Annotations for the Java Platform	Added in Java SE 6, this specification provides annotations for common semantic concepts in the J2SE and J2EE platforms that apply across a variety of individual technologies.
Scripting for the Java Platform	Added in Java SE 6, this specification describes mechanisms allowing scripting language programs to access information developed in the Java Platform and allowing scripting language pages to be used in Java Server-side Applications.

Java Management Extensions (JMX)	The JMX specification provides a management architecture, APIs and services for building Web-based, distributed, dynamic and modular solutions to manage Java enabled resources.
Java Naming and Directory Interface (JNDI)	The Java Naming and Directory Interface (JNDI) provides naming and directory functionality to applications written in the Java programming language. It is defined to be independent of any specific directory service implementation.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Java EE

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.4.2	2/6/2002		
5 (aka 1.5)	9/30/2004		

6 (aka 1.6)	12/11/2006		

VA Forecast Information (11/23/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.4.2	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
5 (aka 1.5)	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
6 (aka 1.6)	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment development and deployment of Java SE is currently based on version 5.0.

General Analysis

Architectural Area

- Application
- Data
- Integration

Architectural Benefits

- Java is a development language that is independent of the operating system
- Java provides virtual machine approach to platform independence
- Java is standards based
- Java is an object-oriented programming language

Architectural Risks

- A security flaw may be exposed in the Java SE platform; however the possibility is

remote considering the excellent security history of the software.

Tier Used

- Middle Tier (Integration)
- Middle Tier (Business)
- Presentation Tier (Thick)
- Client Tier
- Middle Tier (Infrastructure)
- Data Tier

Tool Type

- Platform
- Framework
- Tool

Tool Usage

- Development
- Runtime - Embedded
- Runtime

General Assessment

Expected Usage:	Industry standard object oriented development language and runtime environment.
Assessment Type:	Refresh
Assessment Date:	9/23/2008
Notes:	Approval of this standard does not imply that any reference implementation of this standard is also approved for use.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Java (Java SE) is a foundational platform in the HealtheVet architecture and is essential to the enterprise. Many desktop and browser-based applications depend on the Java SE runtime to function.

4.131) JAXB Reference Implementation

General Information

Website:	https://jaxb.dev.java.net
Description:	Provides a reference implementation Java Architecture for XML Binding specification which allows for marshaling and un-marshaling of Java Objects to XML. This implementation is part of Glassfish a reference implementation of the Java Enterprise Edition standards. The reference implementation can be used independently in applications requiring the ability to marshal and un-marshal Java Object to XML.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	Sun Microsystems

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris

- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- Castor XML
- XMLBeans

Companion Technologies/Standards:

- JAXP Reference Implementation related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0.6	6/26/2006		
2.0.3	10/15/2006		
2.0.5	1/22/2007		
2.1.3	4/13/2007		
2.1.4	7/11/2007		
2.1.5	9/18/2007		
2.1.6	12/19/2007		
2.1.7	5/13/2008		
2.1.8	9/1/2008		

VA Forecast Information (09/26/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008				CY2009				CY2010			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2.0.5	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
2.1.5	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment development and deployment of JAXB is currently based on version 2.1.

General Analysis

Architectural Area

- Application
- Data
- Integration

Architectural Benefits

- Supports XML Schema and DTD
- Provides a standards based framework for marshalling/un-marshalling Java Object State to/from XML

Architectural Risks

- Performance: marshaling large XML files may be too slow for some applications.

Standards Traceability

- XML DTD
- Java EE - JAXB 2.0/2.1
- W3C XML Schema

Tier Used

- Middle Tier (Infrastructure)
- Client Tier
- Data Tier
- Presentation Tier (Web)
- Middle Tier (Business)
- Middle Tier (Integration)

Tool Type

- Framework

Tool Usage

- Development
- Runtime - Embedded

General Assessment

Expected Usage:	Marshal-unmarshal XML to-from Java Objects
Assessment Type:	Refresh
Assessment Date:	9/26/2008
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	JAXB is a standards-based reference implementation.

4.132) JAXP Reference Implementation

General Information

Website:	https://jaxp.dev.java.net
Description:	Reference implementation of the Java API for XML Processing (JAXP) specification for parsing, validating, processing, and querying XML documents with Java. The JAXP reference implementation is a part of the Sun Java SDK and is developed as part of the Glassfish project a reference implementation of the Java Enterprise Edition standards. The JAXP specification is a part of the Java Enterprise Edition Standards.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB

Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	Sun Microsystems

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- JAXB Reference Implementation related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.3	12/16/2005	2/12/2008	
1.3.1	12/16/2005	2/12/2008	
1.3.2	2/18/2006	2/12/2008	
1.4	10/31/2006		
1.4.1	3/20/2007		
1.4.2	5/30/2007		

VA Forecast Information (09/29/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008				CY2009				CY2010			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.3.2	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.4.2	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment development and deployment of JAXP is currently based on version 1.2.

General Analysis

Architectural Area

- Integration
- Application

Standards Traceability

- Java EE - JAXP implements the JAXP 1.3 specification.
- Java EE - JAXP implements the JAXP 1.4 specification.
- JAXP is the reference implementation, implemented as part of JSR-000206 Java API for XML Processing

Tier Used

- Middle Tier (Infrastructure)
- Client Tier
- Presentation Tier (Web)
- Middle Tier (Business)
- Middle Tier (Integration)

Tool Type

- Framework

Tool Usage

- Development
- Runtime - Embedded

General Assessment

Expected Usage:	To parse, validate and process XML documents within the Java applications.
Assessment Type:	Refresh
Assessment Date:	9/29/2008
Notes:	JAXP refers to both a specification and a reference implementation. In this case this entry is focused on the reference implentation.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	JAXP is a standard component in the Java SE platform. It is the reference implentation of the JAXP specification. It is a mature and stable framework with wide adoption in the industry.

4.133) JPEG

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18902

Description: Specifies processes for converting source image data to compressed image data, processes for converting compressed image data to reconstructed image data, coded representations for compressed image data, and gives guidance on how to implement these processes in practice. Is applicable to continuous-tone - grayscale or color - digital still image data and to a wide range of applications which require use of compressed images. Is not applicable to bi-level image data.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Requirements and guidelines	
Compliance testing	
Extensions	

Registration of JPEG profiles, SPIFF profiles, SPIFF tags, SPIFF colour spaces, APPn markers, SPIFF compression types and Registration Authorities (REGAUT)	

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	888: Content Rendering

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1999	1/1/1999		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1999	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.134) JPEG 2000

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=37674

Description: JPEG 2000 defines a set of lossless (bit-preserving) and lossy compression methods for coding bi-level, continuous-tone gray-scale, palletized color, or continuous-tone color digital still images.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Core coding system	
Extensions	This document specifies: • extended decoding processes for converting compressed image data to reconstructed image data • an extended codestream syntax • an extended file format • a container to store image metadata • defines a standard set of image metadata • provides guidance on extended encoding processes for converting source image data to compressed image data • provides guidance on how to implement these processes in practice
Motion JPEG 2000	This document specifies the use of the wavelet-based JPEG 2000 codec for the coding and display of timed sequences of images (motion sequences), possibly combined with audio, and composed into an overall presentation. In this specification, a file format is defined, and guidelines for the use of the JPEG 2000 codec for motion sequences are supplied.
Conformance testing	This document specifies the framework, concepts, methodology for testing, and criteria to be achieved to claim compliance with ISO/IEC 15444-1. It provides a framework for specifying abstract test suites and for defining the procedures to be followed during compliance testing.
Compound image file format	This document defines a normative but optional file format for storing compound images using the JPEG 2000 file format family architecture. A compound image is an image that may contain scanned images, synthetic images or both, and that preferably requires a mix of continuous tone and bi-level compression methods. Besides defining a binary container for a mix of continuous-tone and bi-level images, this format defines a composition model that describes how the multiple images are combined to generate a compound image.
Secure JPEG 2000	This document defines: • a normative codestream syntax containing information for interpreting

	secure image data • a normative process for registering JPSEC tools with a registration authority delivering a unique identifier • informative examples of JPSEC tools in typical use cases • informative guidelines on how to implement security services and related metadata
Extensions for three-dimensional data	This document defines a set of lossless (bit-preserving) and lossy compression methods for coding continuous-tone, bi-level, grey-scale, colour digital volumetric images, or multi-component volumetric images. This set of methods extends the elements in the core coding system defined in ISO/IEC 15444-1 and ISO/IEC 15444-2.
Wireless	This document provides a syntax that allows JPEG 2000 coded image data to be protected for transmission over wireless channels and networks. Protection services include error detection and correction capability for header and bitstream, description of the error sensitivity of different portions of the compressed data, and description of possible residual errors in the compressed data. The syntax allows these protection services to be applied to coded image data in part or in their entirety.
ISO base media file format	This document specifies the ISO base media file format, which is a general format forming the basis for a number of other more specific file formats. This format contains the timing, structure, and media information for timed sequences of media data, such as audio/visual presentations.
Interactivity tools, APIs and protocols	This document defines, in an extensible manner, syntaxes and methods for the remote interrogation and optional modification of JPEG 2000 codestreams and files.

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2000	1/1/2000		
2004	1/1/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2004	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.135) JRules Business Rules Management Server

General Information

Website: http://www.ilog.com/products/jrules/index.cfm

Description: JRules is a commercial Java Business Rules Management System

(BRMS) providing full lifecycle business rules development, testing, deployment and management of rule-sets integrated into java based applications.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: ARB

Decision Process: TRM v3.1

Decision Date: 5/13/2009

Current Status: Introduced

Introduced By: TRM Team

Vendor Name: ILOG

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Business Logic	890: Platform Independent Technologies

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***
- WebLogic Server - ***(required for some configurations)***
- Oracle Database - ***(required for some configurations)***
- SQL Server - ***(required for some configurations)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- JRules Rule Execution Server related as: (Suite)
- JRules Scenario Manager related as: (Suite)
- JRules Rule Studio related as: (Suite)
- JRules Team Server related as: (Suite)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
6.5	2/12/2007		
6.6	10/9/2007		
6.7	2/19/2008		

VA Forecast Information (04/24/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
6.7	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

Forecast Note:	IBM Purchased ILOG in January, 2009, this may impact future versioning and planned releases. Based on past release schedules a new release

	6.8 should have been available in February of 2009, but has not been announced. The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment development and deployment of JRules is currently based on version 6.7.1.

General Analysis

Architectural Benefits

- Integration of a Business Rules Management System provides greater flexibility in externalizing frequently changing business rules. This improves agility and allows applications and the business to respond to changes much quicker.
- As the VA moves to Service Oriented Architecture a Business Rules Management System will play a greater role in business process and service orchestration.

Architectural Risks

- ILOG was purchased by IBM in January of 2009. As IBM looks to integrate ILOG JRules into their current products the focus of ILOG JRules will be on Websphere. Though ILOG JRules does support the Java Rules Specification 94 some functionality requires native access. As IBM and ILOG focus on Websphere there may be integration challenges with other J2EE platforms such as WebLogic in the future.
- Though Java Rules Specification 94 provides guidelines for rule administration and rule runtime APIs providing a standard mechanism for integrating 3rd party rules engines, vendors still use proprietary languages to define rules and actions. This results in rule language lock-in not unlike choosing to implement an application in Java or .Net.

Standards Traceability

- JSR-94 Java Rule Engine API Specification

Tier Used

- Middle-Tier (Business)

Tool Type

- Platform

Tool Usage

- Development
- Management/Collaboration
- Runtime

General Assessment

Expected Usage:	To provide a complete business rules management solution that supports the full lifecycle development of business rules that improve VA agility.
Assessment Type:	New
Assessment Date:	4/27/2009
Notes:	The VA may benefit from a more detailed comparative needs analysis of the top modern Business Rules Management Systems such as Blaze, QuickRules and this entry (JRules). Drools which is an open source BRMS has been requested and needs to be addressed
Recommendation:	Approve
Recommendation Constraints:	None identified at this time.
Recommendation Justification:	Currently the VA does not have an approved Business Rules Management System (BRMS). ILOG JRules is one of the most widely used and robust BRMS. With the recent acquisition by IBM it will continue to mature. Approval is recommended for JRules.

4.136) JRules Rule Execution Server

General Information

Website:	http://www.ilog.com/products/jrules/server.cfm
Description:	J2SE/J2EE compliant execution environment for deployment and operation of applications leveraging external business rules.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v3.1
Decision Date:	5/13/2009
Current Status:	Introduced
Introduced By:	TRM Team
Vendor Name:	ILOG

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	873: Application Servers

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***
- WebLogic Server - ***(required for some configurations)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- JRules Business Rules Management Server related as: (Suite)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (04/24/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	This tool is part of a suite. Please refer to JRules Business Rules Management Server for the VA Forecast.

General Analysis

General Assessment

Expected Usage:	Part of an overall Business Rules Management System to externalize operational rules from VA software products.
Assessment Type:	New
Assessment Date:	4/27/2009
Notes:	Please refer to the technology entry JRules Business Management System for more information.
Recommendation:	Approve
Recommendation Constraints:	None indentified at this time.
Recommendation Justification:	This technology is part of the JRules Business Rules Management System. As part of the overall solution a server for rules execution is critical. Please refer to the JRules Business Rules Management System for recommendation for more detail.

4.137) JRules Rule Studio

General Information

Website: http://www.ilog.com/products/jrules/rulestudio.cfm

Description: An Eclipse-based Integrated Development Environment (IDE) for development of rules based applications. Provides co-editing of rules and java code as well as deployment and debugging of defined rule-sets to the Rule Execution Server. It integrates with the Rule Team Server to provide collaborative development with business rules authors.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: ARB

Decision Process: TRM v3.1

Decision Date: 5/13/2009

Current Status: Introduced

Introduced By: TRM Team

Vendor Name: ILOG

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	867: Integrated Development Environments (IDE)

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRules Rule Execution Server - ***(required for some configurations)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- JRules Team Server related as: (Companion)
- JRules Business Rules Management Server related as: (Suite)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (04/24/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	This tool is part of a suite. Please refer to JRules Business Rules Management Server for the VA Forecast.

General Analysis

General Assessment

Expected Usage:	To provide an integrated development environment (IDE) to define business rules.
Assessment Type:	New
Assessment Date:	4/27/2009
Notes:	Please refer to the technology entry JRules Business Management System for more information.
Recommendation:	Approve
Recommendation Constraints:	None identified at this time.
Recommendation Justification:	This technology is part of the JRules Business Rules Management System. As part of the overall solution it is recommended that a integrated development environment (IDE) be included. Though it is possible to develop rules without an IDE, it is not recommended. Please refer to the JRules Business Rules Management System for recommendation for more detail.

4.138) JRules Scenario Manager

General Information

Website:	http://www.ilog.com/products/jrules/rsm/index.cfm
Description:	Provides rule-set and business simulation unit, regression, functional and impact analysis testing capabilities. Provides facilities for both developer and business user testing.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB

Decision Process:	TRM v3.1
Decision Date:	5/13/2009
Current Status:	Introduced
Introduced By:	TRM Team
Vendor Name:	ILOG

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	869: Test Management

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRules Rule Execution Server - ***(required for some configurations)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- JRules Business Rules Management Server related as: (Suite)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (04/24/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	This tool is part of a suite. Please refer to JRules Business Rules Management Server for the VA Forecast.

General Analysis

General Assessment

Expected Usage:	To test rule-sets implementing in JRules BRMS prior to deployment.
Assessment Type:	New
Assessment Date:	4/27/2009
Notes:	Please refer to the technology entry JRules Business Management System for more information.
Recommendation:	Approve
Recommendation Constraints:	None identified at this time.

Recommendation Justification:	This technology is part of the JRules Business Rules Management System. As part of the overall solution a framework for testing rule-sets and conducting business simulation will provide insure proper rules behavior when deploy to a product environment. Please refer to the JRules Business Rules Management System for recommendation for more detail.

4.139) JRules Team Server

General Information

Website:	http://www.ilog.com/products/jrules/ruleteam.cfm
Description:	Provides a rule repository and management server for authoring, managing, validating and deploying business rules. It is a collaborative environment for rules management.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v3.1
Decision Date:	5/13/2009
Current Status:	Introduced
Introduced By:	TRM Team
Vendor Name:	ILOG

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and	Software Engineering	868: Software Configuration Management

Infrastructure		

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- JRules Rule Studio related as: (Companion)
- JRules Business Rules Management Server related as: (Suite)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (04/24/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010	CY2011	CY2012

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	This tool is part of a suite. Please refer to JRules Business Rules Management Server for the VA Forecast.

General Analysis

General Assessment

Expected Usage:	To provide a collaborative development environment for defining business rules. Also to provide a repository for storage and versioning of business rules.
Assessment Type:	New
Assessment Date:	4/27/2009
Notes:	Please refer to the technology entry JRules Business Management System for more information.
Recommendation:	Approve
Recommendation Constraints:	None identified at this time.
Recommendation Justification:	This technology is part of the JRules Business Rules Management System. As part of the overall solution a repository for storage and versioning of rules is important. Business Rules is a collaborative effort and a platform that supports collaboration is highly desirable. JRules Team Server provides both a repository and a collaborative environment for rules development. Please refer to the JRules Business Rules Management System for recommendation for more detail.

4.140) JUnit

General Information

Website:	http://www.junit.org
Description:	JUnit is a Java unit test development and testing framework. It provides a framework for developers to rapidly develop and deploy unit tests for their Java development artifacts.
Decision:	Approved

Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	SourceForge

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	869: Test Management

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.8.2	3/3/2006		
4.0	2/16/2006		
4.1	4/27/2006		
4.2	11/16/2006		
4.3.1	3/28/2007		
4.4	7/18/2007		
4.5	8/8/2008		
4.6	4/14/2009		
4.7	8/4/2009		

VA Forecast Information (09/09/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
3.8.2	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
4.5	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
4.6	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
4.7	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. The Benefits Segment use of Junit is currently based on version 3.8.1.

General Analysis

Architectural Benefits

- Test Driven Development provides greater application and architectural stability
- A standards based framework for writing and executing java based unit tests

Architectural Risks

- None significant

Tool Type

- Framework
- Tool

Tool Usage

- Development

General Assessment

Expected Usage:	Unit test Java code as part of a test-driven development strategy.
Assessment Type:	Refresh
Assessment Date:	9/26/2008
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Continue use of JUnit.

4.141) Key Management Using ANSI X9.17

General Information

Website:	http://csrc.nist.gov/publications/PubsFIPSArch.html
Description:	Key Management Using ANSI X9.17 provides cryptographic key management guidance. It consists of three parts. Part 1 provides general guidance and best practices for the management of cryptographic keying material. Part 2 provides guidance on policy and security planning requirements for U.S. government agencies. Finally, Part 3 provides guidance when using the cryptographic features of current systems.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	NIST

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Application-Specific Key Management Guidance	This document provides guidance when using the cryptographic features of current systems.
Best Practices for Key Management Organization	This document provides guidance on policy and security planning requirements for U.S. government agencies.
General	This document provides general guidance and best practices for the management of cryptographic keying material.

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
FIPS 171	4/1/1972	2/8/2005	
SP 800 57	3/1/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010	CY2011	CY2012

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
FIPS 171	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.142) Keyed-Hash Message Authentication Code (HMAC)

General Information

Website: http://csrc.nist.gov/publications/PubsFIPS.html

Description: The Keyed-Hash Message Authentication Code (HMAC) describes a keyed-hash message authentication code (HMAC), a mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative Approved cryptographic hash function, in combination with a shared secret key.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: NIST

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
198	3/1/2002		
198-1	7/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
198	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.143) Layer Two Tunneling Protocol (L2TP)

General Information

Website: http://tools.ietf.org/html/rfc2661

Description: Layer Two Tunneling Protocol (L2TP) specifies multi-protocol access via PPP. L2TP facilitates the tunneling of PPP packets across an intervening network in a way that is as transparent as possible to both end-users and applications.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2661	8/1/1999		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be

supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2661	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.144) Lightweight EAP (LEAP)

General Information

Website:

Description:

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name:

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.145) LiveCycle

General Information

Website: http://www.adobe.com/products/livecycle/

Description: The Adobe LiveCycle software is an integrated server solution that blends data capture, information assurance, document output, process management, and content services to help create and deliver Java based applications

Decision: Approved

Decision Constraints: Only the following LiveCycle components have been approved for use:

- Forms ES
- Output ES
- Reader Extensions ES
- Workbench ES
- LiveCycle ES SDK

Decision Source: Benefits Arch

Decision Process: TRM v4.1

Decision Date: 10/28/2009

Current Status: Pending Analysis

Introduced By: Benefits ASA

Vendor Name: Adobe

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	895: Middleware
Service Platform and Infrastructure	Software Engineering	867: Integrated Development Environments (IDE)

Operating Systems Supported

- AIX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***
- WebLogic Server - ***(required libraries)***
- Oracle Database - ***(required for some configurations)***
- Eclipse - ***(required for some configurations)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Flex SDK related as: (Companion)
- Quartz Enterprise Job Scheduler related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
7.2	5/1/2006	6/30/2001	6/30/2013
8.0.1	7/18/2007	7/31/2012	7/31/2014
8.1.1	3/5/2008		
8.2	7/1/2008		
8.2.1	2/1/2009		

VA Forecast Information (09/27/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
8.0.1	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
8.2	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.146) Local Area Network (LAN)

General Information

Refer to document: VA_Enterprise_IT_Infrastructure_Standard_LAN_1_0.pdf

Description: This standards document lists the acceptable and recommended specifications for Local Area Network. Sections include standard specifications for subject components, decisions supporting the standard specifications, guidelines or recommendations for implementing the standard specifications, and supplemental factors to consider when evaluating subject components. Other supplementary documents will provide guidance on procuring components that meet the standard specifications, guidance on integrating them with existing components, and explanation of how the subject components fit into the VA Architecture.

This standard includes the following: CORE Network Switch; End-of-Row Access Layer Switch; High-Bandwidth Converged I/O Access Layer Switch; VistA Private SCS DCI Router/Switch; Blade Server Chassis Access Layer Switch; Management Access Layer Switch; Load Balancer.

For each of these standards the following supporting details are included; Chassis, Packet Processor, Linecards/Port Interfaces, Operating System, Support, and High Availability.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EIE CTO

Decision Process: TAR-TAS

Decision Date: 11/5/2009

Current Status: Analysis Completed

Introduced By: OPS/EIE

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code

Service Platform and Infrastructure	Hardware/Infrastructure	881: Local Area Networks (LAN)

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (09/27/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.147) Log4J

General Information

Website:	http://logging.apache.org/log4j
Description:	Log4J is a Java runtime logging framework that allows developers to include in their source code, the ability to generate logging output messages. The verbosity and output of the log can be controlled by configuration at runtime.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	ASF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	895: Middleware

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- JRE - Sun

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.2.14	9/18/2006		
1.2.15	8/24/2007		

VA Forecast Information (10/01/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008	CY2009	CY2010

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.2.14	Supported	Supported	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.2.15	None	None	None	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. The Benefits Segment use of Log4J is currently based on version 1.2.14.

General Analysis

Architectural Area

- Application
- Integration

Architectural Benefits

- Minimizes the use of System.out and other improper logging approaches.
- Provides a standardize mechanism for logging within applications

Architectural Risks

- None significant

Tier Used

- Middle Tier (Infrastructure)

Tool Type

- Framework

Tool Usage

- Development
- Runtime - Embedded

General Assessment

Expected Usage:	A standard logging framework for Java applications.
Assessment Type:	Refresh
Assessment Date:	9/30/2008

Notes:	Log4J is the de-facto standard for Java application logging. Java SE JDK is an alternative, but lags behind Log4J in maturity and robustness. Log4J can work with and is complementary to the Enterprise Exception Log Service (EELS).
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Recommend continued use of this tool along with EELS.

4.148) Mail Services

General Information

Description:	Mail services pass messages between Message Transfer Agent (MTA) - a program that is responsible for either delivering the message locally or passing it to another MTA, often on another host. MTAs on different hosts on a network often communicateusing SMTP. The message is eventually delivered to the recipient's mailbox - normally a file on his computer - from where he can read it using a mail-reading program (which may or may not be the same Mail User Agent (MUA) as used by the sender).
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description

Internet/Intranet Services	VA Handbook 6102	This Handbook provides procedures relating to the establishment and administration of a VA Internet and/or Intranet site, and/or site operating on behalf of VA, and/or related service; it also provides procedures for publishing VA information on the World Wide Web (www).

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
IETF RFC 1957	Some Observations on Implementations of the Post Office Protocol (POP3)

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	871: Web Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.149) Malicious Code Detection

General Information

Description: Malicious Code Detection (anti-virus or virus checking programs) services monitor for viruses and may take action to remove or isolate the virus, preventing it from executing and spreading.

Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Anti-virus software installation		All PC-based workstations and servers (including those using the Windows, Linux, Unix (all variants), and Macintosh operating systems) shall employ anti-virus software.
Anti-virus software updates		Updated virus detection signatures shall be downloaded and installed at least monthly.
Anti-virus software configuration		Anti-virus software shall be configured to run in a background mode.
Virus scanning		Procedures shall be implemented requiring files to be virus scanned: • incoming to the computer system (e-mail, floppy, CD, FTP, etc.) • before they are attached to outgoing e-mail. A record of the time and date of the scan as well as the tool used should be included in the body of the e-mail. • upon access • on a regularly scheduled basis
Blocking .exe files		Executable files from questionable sources, such as electronic greeting cards and shareware downloads, should be blocked at the external gateways because they may contain malicious software.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Technical Cyber Security Alerts	Technical Cyber Security Alerts provide timely information about current security issues, vulnerabilities, and exploits.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Security Controls*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.150) Management Information Base (MIB)

General Information

Website:	http://tools.ietf.org/
Description:	Management Information Base (MIB) is a type of database used for managing the devices in a communications network. It comprises a collection of objects in a (virtual) database used to manage entities (such as routers and switches) in a network.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2

Decision Date: 3/14/2008
Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Structure and Identification of Management Information for TCP/IP-based Internets	This document provides the common definitions for the structure and identification of management information for TCP/IP-based internets.
MIB for TCP/IP	
MIB for SNMP	This document defines managed objects which describe the behavior of a Simple Network Management Protocol (SNMP) entity.
Entity MIB (Version 3)	This document describes managed objects used for managing multiple logical and physical entities managed by a single SNMP agent.
Entity State MIB	This document defines a set of Textual Conventions to represent various states of an entity.
Alarm Management Information Base (MIB)	This document describes management objects used for modelling and storing alarms.
MIB for UDP	This document describes managed objects used for implementations of the User Datagram Protocol (UDP) in an IP version independent manner.
MIB for IP	This document describes managed objects used for implementations of the Internet Protocol (IP) in an IP version independent manner.
Remote Network Monitoring MIB	This document defines objects for managing remote network monitoring devices.
MPLS FEC-To-NHLFE MIB	This document describes managed objects for defining, configuring, and monitoring Forwarding Equivalence Class (FEC) to Next Hop Label Forwarding Entry (NHLFE) mappings and corresponding actions for use with Multiprotocol Label Switching (MPLS).

Definitions of Managed Objects for MPLS LDP	This document defines a portion of the Management Information Base (MIB)

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (10/01/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. The Benefits Segment use of Log4J is currently based on version 1.2.14.

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.151) Media Servers

General Information

Description:	Provide optimized management of media based files such as audio and videostreams and digital images.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.152) Medical Device Interoperability

General Information

Description:	Medical Device Interoperability standards allow for health care providers to plug medical or point of care devices into information and computer systems that allows health care providers to monitor information from inpatient bedside or home healthcare environments (a.k.a. Tele-medicine).
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Applicability	Standard for Medical Device Communications (IEEE 1073) should be adhered to when the application is hosted on micro-controller platform, not a PC or server-based platform.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	878: Embedded Technology Devices

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.153) Medical Radiology Images Exchange

General Information

Description: Medical/Radiology Images Exchange standards facilitate interoperability of diagnostic medical imaging equipment by specifying: (a) A set of protocols to be followed by devices, (b) The syntax and semantics of Commands and associated information, and (c) Information that must be supplied with an implementation.

Decision: Approved

Decision No constraints have been specified at this time.

Constraints:

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Clinical Images	DICOM and JPEG-2000 formats should be used to exchange clinical images between imaging systems.
Health Information	HL7 messages should be used to exchange data between imaging systems and health information systems.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.154) Metropolitan Area Network Services

General Information

Description: Metropolitan area network (MAN) services provide access between networks in a metro region.The MAN is the network that picks up traffic from the LAN and passes it to another LAN in the same metro area or to the WAN. The MAN can be described in terms of distance and function. Interms of distance, LANs typically span fewer than two kilometers while MANs can cover distances of up to 150 kilometers. In contrast, the WAN extends beyond the MAN, typically spanning farther than 150 km. In terms of function, a goal of MAN services is to provide secure distributed broadband access to end-users.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Fiber Optic Cables		Fiber optic cabling shall be used for connectivity between MANs and LANs

Guidelines and Best Practices

No guidelines have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and	Hardware/Infrastructure	Metropolitan Area Network (MAN)*

Infrastructure		

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.155) Mirth Connect

General Information

Website:	http://www.mirthcorp.com/products/mirth-connect
Description:	Mirth Connect is an open source cross-platform healthcare integration engine that supports the creation of interfaces, or channels, that perform message filtering, transforming, and routing between disparate systems.
Decision:	Approved
Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	Mirth Corp.

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	896: Enterprise Application Integration

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- BusinessWare
- Mirth Connect

Companion Technologies/Standards:

- Transmission Control Protocol (TCP) related as: (Companion)
- Internet Protocol (IP) related as: (Companion)
- File Transfer Protocol (FTP) related as: (Companion)
- Simple Object Access Protocol (SOAP) related as: (Companion)
- HL7 related as: (Companion)
- XSL Transformations (XSLT) related as: (Companion)
- Digital Imaging and Communications in Medicine (DICOM) related as: (Companion)

- Portable Document Format (PDF) related as: (Companion)
- Rich Text Format (RTF) related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.6	8/16/2006		
1.7	4/25/2008		
1.8	1/15/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.6	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.156) MPEG-1

General Information

Website:	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=19180
Description:	ISO/IEC 11172: Motion Picture Experts Group (MPEG-1) defines a coding standard of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Systems	This document specifies the system layer of the coding. The specification was developed principally to support the combination of the video and audio coding methods defined in ISO/IEC 11172-2 and ISO/IEC 11172-3. The system layer supports the following basic functions: the synchronization of multiple compressed streams on playback, the interleaving of multiple compressed streams into a single stream, the initializiation of buffering for playback start up, continuous buffer management, and time identification.
Video	This document specifies the coded representation of video for digital storage media and the decoding process. It is primarily applicable to digital storage media supporting a continuous transfer rate up to about 1,5 Mbit/s, such as compact disc, digital audio tape, and magnetic hard disc, and for non-interlaced video formats having approximately 288 lines of 352 pels and picture rates around 24 Hz to 30 Hz. Nevertheless it can be used more widely than this because of the generic approach taken.

Audio	This document specifies the coded representation of high quality audio for storage media and the method for decoding of high quality audio signals. Is intended for application to digital storage media providing a total continuous transfer rate of about 1,5 Mbit/s for both audio and video bitstreams, such as CD, DAT and magnetic hard disc, and for sampling rates of 32 kHz, 44,1 kHz, and 48 kHz.
Compliance Testing	This document specifies how tests can be designed to verify whether bitstreams and decoders meet requirements specified in parts 1, 2 and 3 of ISO/IEC 11172. Summarizes the requirements, cross references them to characteristics, and defines how compliance with them can be tested. Gives guidelines how to construct tests and determine their outcome. Defines some actual tests only for audio.
Software simulation	

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1999	11/15/1999		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1999	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.157) MPEG-2

General Information

Website: http://webstore.ansi.org/RecordDetail.aspx?sku=ISO%2fIEC+13818-2%3a2000&source=google&adgroup=iso9&keyword=iso%2Fiec%2013818-2&gclid=CLmYj-zfqaACFdRM5Qod62kycg

Description: ISO/IEC 13818: Motion Picture Experts Group (MPEG-2) Generic coding of moving pictures and associated audio information: Part 2 - Video, specifies the coded representation of picture information for digital storage media and digital video communication and specifies the decoding process.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Systems	This document specifies the systems layer of the coding. The system layer supports six basic functions: • the synchronization of multiple compressed streams on decoding • the interleaving of multiple compressed streams into a single stream • the initialization of buffering for decoding start up • ontinuous buffer management • time identification • multiplexing and signalling of various components in a system stream
Video	
Audio	
Conformance Testing	This document specifies how tests can be designed to verify whether coded data and decoders meet requirements specified in parts 1, 2, 3 and 7 of ISO/IEC 13818.
Software simulation	This document provides a C language software simulation of an encoder and decoder for Part 1 (Systems), Part 2 (Video), Part 3 (Audio), Part 7 (AAC) and Part 11 (IPMP) of ISO/IEC 13818.
Advanced Audio Coding	This document specifies MPEG-2 Advanced Audio Coding (AAC), a multi-channel audio coding standard that delivers higher quality than is achievable when requiring MPEG-1 backwards compatibility. It provides ITU-R "indistinguishable" quality at a data rate of 320 kbit/s for five full-bandwidth channel audio signals.
IPMP on MPEG-2 systems	This document specifies IPMP (Intellectual Property Management and Protection) on the MPEG-2 system. MPEG-2 IPMP offers flexibility, robustness and interoperability, which allows the secure content delivery in the MPEG-2 system. MPEG-2 IPMP can be used in combination with

	proprietary IPMP tools, which enables the implementation to various degrees of security for different business models, while maintaining the interoperability
Extensions for DSM-CC	
Extensions for real time interface for systems decoders	

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2000	12/1/2000		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different

releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2000	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.158) MPEG-4

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38559

Description: ISO/IEC 14496: Motion Picture Experts Group (MPEG-4) specifies system-level functionalities for the communication of interactive audio-visual scenes. It specifies the following:

- a terminal model for time and buffer management
- a coded representation of metadata for the identification, description and logical dependencies of the elementary streams
- a coded representation object content information, a descriptive audio-visual content information
- an interface to intellectual property management and protection systems
- a coded representation of synchronization information
- a multiplexed representation of individual elementary streams in a single stream

Decision: Approved

Decision No constraints have been specified at this time.

Constraints:

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Systems	This document specifies system-level functionalities for the communication of interactive audio-visual scenes.
Visual	The Visual specification contains definitions of the bitstream syntax, bitstream semantics and the related decoding process. It does not specify the encoders, which can be optimized in different implementations.
Audio	This Audio specification integrates many different types of audio coding: natural sound with synthetic sound, low bitrate delivery with high-quality delivery and lossless coding, speech with music, complex soundtracks with simple ones, and traditional content with interactive and virtual-reality content.
Conformance Testing	This document specifies how tests can be designed to verify whether bitstreams and decoders meet requirements specified in parts 1:Systems, 2:Visual, 3:Audio and 6: DMIF. It specifies how tests can be designed for bitstream delivery over various delivery technologies in an interoperable transparent manner.
Delivery Multimedia Integration Framework (DMIF)	This document specifies an interface between the application and the transport, that allows the MPEG-4 application developer to stop worrying about that transport. A single application can run on different transport layers when supported by the right DMIF instantiation.
Reference Software	This document identifies reference software for demonstrating and clarifying the other parts of the standard.

ptimized reference software for coding of audio-visual objects	This document specifies the encoding tools that enhance both the execution and quality for the coding of visual objects as defined in Visual
Carriage of ISO/IEC 14496 contents over IP networks	This document provides a framework for the carriage of ISO/IEC 14496 contents over IP networks and guidelines for designing payload format specifications for the detailed mapping of ISO/IEC 14496 content into several IP-based protocols.
Reference hardware description	This document specifies descriptions of the main video coding tools in hardware description language (HDL) form.
Advanced Video Coding	This document pecifies advanced video coding for coding of audio-visual objects.
Scene description and application engine	This document specifies the coded representation of interactive audio-visual scenes and applications.
ISO base media file format	This document specifies the ISO base media file format, which is a general format forming the basis for a number of other more specific file formats. This format contains the timing, structure, and media information for timed sequences of media data, such as audio/visual presentations.
Intellectual Property Management and Protection (IPMP) extensions	This document specifies the definition, as well as Extension tags, syntax and semantics for an IPMP_Data_BaseClass.
MP4 file format	This document specifies the MP4 file format as derived from ISO/IEC 14496-12 and ISO/IEC 15444-12, the ISO base media file format.
dvanced Video Coding (AVC) file format	This document specifies how Advanced Video Coding (AVC) streams are stored in file formats derived from ISO/IEC 14496-12 & 15444-12 (The ISO Base Media File Format).
Animation Framework eXtension (AFX)	This document specifies MPEG-4 Animation Framework eXtension (AFX) model for representing and encoding 3D graphics assets to be used standalone or integrated in interactive multimedia presentations (the latter when combined with other parts of MPEG-4).
Streaming text format	This document specifies a text stream as a concatenation of text access units. A text access unit contains text information of a specific format.
Font compression and streaming	This document defines the set of technologies for compression, encoding and delivery of complex audio-visual scenes composed of different media objects.
ynthesized texture stream	This document specifies the transmission of synthesized texture data as part of the MPEG-4 encoded audio-visual presentation.
Lightweight	This document defines a scene description format (LASeR) and an

Application Scene Representation (LASeR) and Simple Aggregation Format (SAF)	aggregation format (SAF) respectively suitable for representing and delivering rich-media services to resource-constrained devices such as mobile phones.
MPEG-J Graphics Framework eXtensions (GFX)	This document describes a lightweight programmatic environment for advanced interactive multi-media applications. Designed for limited resources devices such as mobile phones.
Open Font Format	This document specifies the Open Font Format (OFF) specification, the TrueType and Compact Font Format (CFF) outline formats, and the TrueType hinting language.
ymbolic Music Representation	This document specifies Symbolic Music Representation (SMR).
Audio and systems interaction	This document describes the desired joint behavior of MPEG-4 Systems (MPEG-4 File Format) and MPEG-4 Audio codecs.
3D Graphics Compression Model	This document describes a model for connecting 3D Graphics Compression tools defined in ISO/IEC 14496 to graphics primitives defined in any other standard, specification or recommendation.
3D Graphics conformance	This document specifies how tests can be designed to verify whether compressed data (i.e. bitstreams) and decoders meet the requirements for the synthetic 3D graphics tools specified in ISO/IEC 14496-11, ISO/IEC 14496-16, ISO/IEC 14496-21, and ISO/IEC 14496-25.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2001			
2004			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2004	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.159) Multimedia Transport

General Information

Description: Multimedia transport services provide a convergence of the existing voice, video, and data infrastructures. Toll bypass applications use routers (gateways) to route voice and fax calls from one telephone switch to another using packet networks instead of the traditional switched telephone network. Transporting voice over a common infrastructure allows the VA to route voice calls between medical centers using the WAN, reducing expenditures on costly leased lines and public network calls and minimizing the operational costs of moving telephone equipment as employees move from location to location. A converged infrastructure will become increasingly important as the VA increases its use of telemedicine and tele-radiology applications.

Decision: Approved

Decision Constraints: PBXs that do not support VoIP capability are not approved for VA use.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
PBX Requirements		New PBX equipment shall support detection and blocking of incoming modem calls where not allowed. This should be done using Caller ID, Time restrictions, and destination phone numbers.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
ITU-T T.121	Data protocols for multimedia conferencing - Generic application template
Toll Bypass Capability	PBXs that do not have toll bypass capability should be replaced or upgraded.
QoS	Switches that do not support QoS should be replaced.

PTSN	PBXs should support PSTN backup.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	Multimedia Transport*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.160) Multiplexing Protocol for Low Bit Rate Multimedia Communication

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=H

Description: ITU-T H.223: Multiplexing Protocol for Low Bit Rate Multimedia Communication specifies a packet-oriented multiplexing protocol for low bit rate multimedia communication. This protocol can be used between two low bit rate multimedia terminals, or between a low bit rate multimedia terminal and a multipoint control unit or an interworking adapter. The protocol allows the transfer of any combination of digital voice/audio, digital video/image and data information over a single communication link. This protocol provides low delay and low overhead by using segmentation and reassembly and by combining information from different logical channels in a single packet.

Decision: Approved

Decision No constraints have been specified at this time.

Constraints:	
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2	7/29/2001		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.161) Multipoint Binary File Transfer Protocol

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=T

Description: ITU-T T.127: Multipoint Binary File Transfer Protocol defines a protocol to support the interchange of binary file data within an interactive conferencing or group working environment where the T.120 suite of standards is in use. It provides mechanisms to support simultaneous distribution of multiple files, selective

distribution of files to a subset of participants and retrieval of files from remote sites. Provision is also made for remote directory access.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1	8/11/1995		
2	8/29/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.162) Multipoint Communication Service (MCS) - Service Definition

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=T

Description: ITU-T T.122: Multipoint Communication Service (MCS) – Service Definition defines a multipoint data delivery service for use in the audiographics and audiovisual conferencing service. It provides the mechanism for multipoint aware applications to send data to all or a subset of the group with a single send primitive and to force, if desired, a uniformly sequenced reception of data at all users. It also provides a token mechanism to allow applications to control scarce resources or do multi-application signalling and synchronization. These services are provided in a manner that is independent of the underlying network connections.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2	2/6/1998		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.163) Multipoint Communication Service (MCS) Protocol

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=T

Description: ITU-T T.125: Multipoint Communication Service Protocol Specification defines a protocol operating through the hierarchy of a multipoint communication domain. It specifies the format of protocol messages and procedures governing their exchange over a set of transport connections. The purpose of the protocol is to implement the Multipoint Communication Service defined by ITU-T T.122.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2	2/6/1998		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.164) Multipoint Control Units for Audiovisual Systems

General Information

Website:	http://www.itu.int/itu-t/recommendations/index.aspx?ser=H
Description:	ITU-T H.231: Multipoint Control Units for Audiovisual Systems Using Digital Channels up to 1920 kbit/s specifies the means by which three or more audiovisual terminals conforming to Recommendation ITU-T H.320 may communicate simultaneously over constant bit rate digital paths, such communication being designated a "multipoint call".
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3	7/11/1997		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

3	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.165) Multipoint Still Image and Annotation Protocol

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=T

Description: ITU-T T.126: Multipoint Still Image and Annotation Protocol defines a protocol supporting the management of common multi-layer visual spaces and the multipoint exchange of graphical information directed to these spaces including images (hard and soft copy), pointers, and filled and unfilled parametric drawing elements (points, lines, polygons and ellipses). Support for rendering out-of-band video streams within T.126 workspaces is also included. In addition, keyboard and pointing device exchanges are specified to support basic user interaction. Protocol elements for creating and referencing archived visual spaces are defined to allow pre-stored or pre-distributed graphical materials to be referenced.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Data Protocols for Multimedia Conferencing - Generic Conference Control - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2	7/11/1997		
3	8/29/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the

responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.166) Multiprotocol Label Switching (MPLS) Architecture

General Information

Website: http://tools.ietf.org/html/rfc3031

Description: Multiprotocol Label Switching (MPLS) Architecture is a mechanism in high-performance telecommunications networks which directs and carries data from one network node to the next. MPLS makes it easy to create "virtual links" between distant nodes. It can encapsulate packets of various network protocols.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
MPLS Management Overview	This document describes the management architecture for MPLS and indicates the interrelationships between the different MIB modules used for MPLS network management.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date

RFC 3031	1/1/2001		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
RFC 3031	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.167) Multipurpose Internet Mail Extensions (MIME)

General Information

Website: http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

Description: Multipurpose Internet Mail Extensions (MIME) defines a message representation protocol specifying considerable detail about US-ASCII message headers, and leaves the message content, or message body, as flat US-ASCII text. This set of documents, collectively called the Multipurpose Internet Mail Extensions, or MIME, redefines the format of messages to allow for:

- textual message bodies in character sets other than US-ASCII
- an extensible set of different formats for non-textual message bodies
- multi-part message bodies
- textual header information in character sets other than US-ASCII

Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Format of Internet Message Bodies	This document specifies the various headers used to describe the structure of MIME messages.
Media Type	This document defines the general structure of the MIME media typing system and defines an initial set of media types.
Message Header Extensions for Non-ASCII Text	This document describes extensions to allow non-US-ASCII text data in Internet mail header fields.
Registration Procedures	This document specifies various IANA registration procedures for the following MIME facilities: media types, external body access types, and content-transfer-encodings.
Conformance Criteria and Examples	This document defines a certain level of implementation that allows the useful interworking of messages with content that differs from US-ASCII text.

FEA Categories

Service Area	Service Category	Service Standard Code

Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2045	11/1/1996		
RFC 2231	11/1/1997		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2045	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.168) Narrow-band Visual Telephone Systems and Terminal Equipment

General Information

Website:	http://www.itu.int/itu-t/recommendations/index.aspx?ser=H
Description:	ITU-T H.320: Narrow-band Visual Telephone Systems and Terminal Equipment specifies technical requirements for narrow-band visual telephone systems and terminal equipment, typically for videoconferencing and videophone services. It describes a generic system configuration consisting of a number of elements which are specified by respective ITU-T Recommendations, definition of communication modes and terminal types, call control arrangements, terminal aspects and interworking requirements.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5	3/15/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
5	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.169) Native Audio Formats

General Information

Description: The Native Audio formats service deals with the compression, decompression, processing, and encoding representation of audio.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
CD-ROM	Audio burned onto a CD-ROM should be in an MPEG-1 format.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	Native Audio Formats*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.170) Native Document Formats

General Information

Description:	Native Document formats are the standard internal organization schemes for human-readable documents meant for public distribution.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Web Distribution	Documents that are distributed to the general public over the web should be in a PDF format

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	Native Document Formats*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.171) Native Graphics Formats

General Information

Description:	Native Graphics formats are the standard internal organization schemes for static and interactive two- and three-dimensional images.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision	FA

Source:	
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Thin Client	JPEG is best used for full color “natural” scenes. GIF is best for black & white images or man-made graphics.
Medical	DICOM is the preferred format for medical image exchange.
Vector-based Images	Where applicable, vector-based images should be used as they are scalable without losing detail.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	Native Graphics Formats*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.172) Native Video Formats

General Information

Description: The Native Video formats service deals with the compression, decompression, processing, and coded representation of combined moving pictures and audio.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
CD-ROM	Video burned onto a CD-ROM should be in an MPEG-2 format.
Streaming (High)	Video broadcasted (streaming) over very high bandwidth devices should be in an MPEG-2 format.
Streaming (Low)	Video broadcasted (streaming) over low bandwidth devices should be in an MPEG-4 format.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	Native Video Formats*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.173) Neighbor Discovery for IPv6

General Information

Website:	http://tools.ietf.org/html/rfc2461
Description:	Neighbor Discovery for IP Version 6 (IPv6) specifies the Neighbor Discovery protocol for IP Version 6. IPv6 nodes on the same link use Neighbor Discovery to discover each other's presence, to determine each other's link-layer addresses, to find routers and to maintain reachability information about the paths to active neighbors.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2461	12/1/1998	9/1/2007	
RFC 4311	11/1/2005		
RFC 4861	9/1/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be

supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2461	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.174) NetBackup

General Information

Website: http://www.symantec.com/business/products/family.jsp?familyid=netbackup

Description: NetBackup provides online backup, and recovery of databases and applications; enables backup and recovery operations over storage networks; and delivers high levels of data security and complete system-level recovery.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: CDCO Supported Architecture Components

Vendor Name: Symantec

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date

6.0	10/1/2005		
6.5	8/1/2007		
7.0	2/1/2010		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
6.5	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.175) Network Address Translation - Protocol Translation (NAT-PT)

General Information

Website: http://tools.ietf.org/html/rfc2766

Description: Network Address Translation - Protocol Translation (NAT-PT) specifies an IPv4-to-IPv6 transition mechanism. This solution attempts to provide transparent routing to end-nodes in V6 realm trying to communicate with end-nodes in V4 realm and vice versa.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2766	2/1/2000	7/1/2007	
RFC 4966	7/1/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2766	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.176) Network Transport

General Information

Description: These consist of the protocols that define the format and structure of data and information that is either accessed from a directory or exchanged through communications.
For the transport of data to take place, each communications process must adhere to rules and procedures. Network protocols are the rules and technical procedures that enable application and middleware communications across the network. In a network,

several protocols work together to ensure that the communication is prepared, transferred, received, and acted upon. The work of the Network Protocols must be coordinated so there is no disagreement. To minimize the potential for conflict, protocols operate in layers. Each layer specifies a different function of the communications process. The lower layer protocols specify how vendors can make their equipment connect to other equipment. Middle layer protocols provide session capability for the middleware layer and ensure that the data is able to move reliably between network devices. The upper layer protocols specify rules for application-to-application interaction.
The TCP/IP protocol suite enables transport, file transfer, terminal emulator, messaging, e-mail, and network management capabilities for core infrastructure system services at the middleware and application layers. The Hypertext TransferProtocol (HTTP), an application level protocol, is the enabler for World Wide Web access.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.177) Network-specific Data Protocol Stacks for Multimedia Conferencing

General Information

Website:	http://www.itu.int/itu-t/recommendations/index.aspx?ser=T
Description:	ITU-T T.123: Network-specific Data Protocol Stacks for Multimedia Conferencing specifies network specific aspects of the T.120-series data protocols for multimedia conferencing. The networks currently identified are ISDN, CSDN, PSDN, PSTN, BISDN, and LAN. Communication profiles are specified which provide reliable point-to-point connections between a terminal and a multipoint control unit, between pairs of terminals or between pairs of MCUs. In some cases, a lower protocol layer allows the multiplexing of audio and video signals in addition to data connections. In other cases, separate calls, over the same or a different network, may be established to carry audio or video signals.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
4	5/27/1999		
5	1/13/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
4	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.178) Object Linking and Embedding, Database (OLE DB)

General Information

Website: http://msdn.microsoft.com/en-us/library/ms722784%28VS.85%29.aspx

Description: Object Linking and Embedding, Database (OLE DB) is a set of Component Object Model (COM) interfaces that provide applications with uniform access to data stored in diverse information sources and that also provide the ability to implement additional database services. These interfaces support the amount of DBMS functionality appropriate to the data store, enabling it to share its data.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008
Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: Microsoft

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Management	893: Database Connectivity

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Open Database Connectivity (ODBC)

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date

Vendor release information is not available for this entry.

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	See ODBC for forecast information.

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.179) Objects and Attributes for Access Control

General Information

Website:	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18166
Description:	ISO/IEC 10164-9 & ITU-T X.741: Objects and Attributes for Access Control describes an Access Control Security Model and the management information necessary for creating and administering access control associated with OSI System Managements. Security policy adoped for any instance of use is not specified and is left as an implementation choise. This Specification is of generic application and is applicable to the security management of many types of application.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.

Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1995 (1.0)	4/10/1995		
1996 (1.1)	10/5/1996		
1999 (1.2)	6/26/1998		
2002 (1.3)	2/4/2000		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2002 (1.3)	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.180) Office Open XML

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51463

Description: ISO/IEC 29500: Office Open XML defines a set of XML vocabularies for representing word-processing documents, spreadsheets and

presentations, based on the Microsoft Office 2008 applications. It specifies requirements for Office Open XML consumers and producers that comply to the strict conformance category.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	Native Document Formats*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Portable Document Format (PDF)
- Rich Text Format (RTF)

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2008			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2008	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.181) Open Database Connectivity (ODBC)

General Information

Website: http://msdn.microsoft.com/en-

us/library/ms710252%28VS.85%29.aspx

Description: Open Database Connectivity (ODBC) is an application programming interface (API) specification for database access. It is based on the Call-Level Interface (CLI) specifications from Open Group and ISO/IEC for database APIs and uses Structured Query Language (SQL) as its database access language.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: Microsoft

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Management	893: Database Connectivity

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Java SE

Companion Technologies/Standards:

- Object Linking and Embedding, Database (OLE DB) - Standard
- Common Language Infrastructure (CLI) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.5	1/1/1997		
3.8	1/1/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
3.5	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.182) Open Graphics Library (OpenGL)

General Information

Website:	http://www.opengl.org/registry/
Description:	OpenGL (Open Graphics Library) is a standard specification defining a cross-language, cross-platform API for writing applications that produce 2D and 3D computer graphics.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	OpenGL

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2.1	7/2/2006		
3.0	7/11/2008		
3.1	5/28/2009		
3.2	8/3/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
3.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
3.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.183) Open Shortest Path First (OSPF) Protocol

General Information

Website:	http://tools.ietf.org/html/rfc2328
Description:	Open Shortest Path First (OSPF) Protocol is a specification of the Open Shortest Path First (OSPF) internet routing protocol. OSPF is classified as an Internal Gateway Protocol (IGP).
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code

Service Access and Delivery	Service Transport	IP Routing Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2328	4/1/1998		
RFC 5709	10/1/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2328	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.184) OpenVMS

General Information

Website:	http://h71000.www7.hp.com/openvms/operatingsystem.html
Description:	OpenVMS is a general-purpose, multi-user operating system. It has well-integrated networking, distributed computing, client/server, multiprocessing, and windowing capabilities.
Decision:	Approved
Decision Constraints:	Products that have been deployed to a production environment may continue to use this technology. All other products must utilize a One-VA TRM approved Linux operating system.
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	HP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	866: Dependent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
7.3.1	8/1/2002		3/31/2005
8.0	6/1/2003		
8.1	12/1/2003		
8.2	1/1/2005		
8.3	10/1/2007		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
7.3.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.185) Oracle Database

General Information

Website: http://www.oracle.com/database/index.html

Description: The Oracle relational database management system. There are several Oracle editions (Express, Personal, Standard, Enterprise, and Real Application Cluster). This assessment is concerned with the Standard and Enterprise editions of Oracle.

Decision: Approved

Decision Constraints: Benefits Segment development and deployment of Oracle is limited for use only within the Corporate Database

Decision Source: ARB

Decision Process: TRM v2

Decision Date: 9/17/2008

Current Status: Analysis Completed

Introduced By: Extended Tool List (ETL)

Vendor Name: Oracle

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Database/Storage	875: Database

Operating Systems Supported

- AIX
- HP-UX
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Structured Query Language (SQL) - ***(required for some configurations)***

Comparable Technologies/Standards:

- Cache Database Engine
- SQL Server

Companion Technologies/Standards:

- Oracle JDBC Drivers related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
8.1	4/1/1999		
9.2	3/1/2002		
10.1	5/1/2004		

10.2	5/1/2005		
11.1	5/1/2007		
11.2	9/1/2009		

VA Forecast Information (04/09/2010)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
8.1	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
9.2	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
10.2	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
11.1	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment development and deployment of Oracle Database is currently based on version 10.2.

General Analysis

Architectural Area

- Data

EA Requirement

- ENTR 1074 - Implement a One VA information technology framework that supports the integration of information across business lines and that provides a source of consistent, reliable, accurate, and secure information to veterans and their families, employees, and stakeholders (Enabling Objective E-3).
- ENTR 239 - VA Enabling Goal - Deliver World-Class Service: Deliver world-class service to veterans and their families by applying sound business principles that result in effective management of people, communications, technology, and governance.

Standards Traceability

- ANSI SQL 92

Tier Used

- Data Tier

Tool Type

- Framework
- Tool
- Platform

Tool Usage

- Development
- Management/Collaboration
- Runtime

General Assessment

Expected Usage:	Provide an enterprise class commercial relational database management system with the ability to store and retrieve veterans' information securely and reliably.
Assessment Type:	Refresh
Assessment Date:	9/18/2008
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Continue using Oracle as the production database.

4.186) Oracle RAC

General Information

Website:	http://www.oracle.com/technology/products/database/clustering/inde

x.html

Description: Oracle Real Application Clusters (RAC) is a cluster database with a shared cache architecture that provides highly scalable and available database solutions.
Oracle RAC is an option of the Oracle Database Enterprise Edition.

Decision: Approved

Decision Constraints: Benefits Segment development and deployment of Oracle is limited for use only within the Corporate Database

Decision Source: Benefits Arch

Decision Process: TRM v4.1

Decision Date: 10/28/2009

Current Status: Pending Analysis

Introduced By: Benefits ASA

Vendor Name: Oracle

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Database/Storage	875: Database

Operating Systems Supported

- AIX
- HP-UX
- Solaris
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Oracle Database - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information ()

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	Refer to Oracle Database for VA version forecast details regarding this technology.

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.187) Packet-Based Multimedia Communications Systems

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=H

Description: ITU-T H.323: Packet-Based Multimedia Communications Systems describes terminals and other entities that provide multimedia communications services over Packet-Based Networks (PBN) which may not provide a guaranteed Quality of Service. H.323 entities may provide real-time audio, video and/or data communications. Support for audio is mandatory, while data and video are optional, but if supported, the ability to use a specified common mode of operation is required, so that all terminals supporting that media type can interwork.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
6	6/13/2006		
7	12/14/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
6	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.188) Parallel Sysplex

General Information

Website: http://www-03.ibm.com/systems/z/advantages/pso/index.html

Description: Parallel Sysplex is a clustering technology. It allows IBM mainframes to act together as a single system image with z/OS. Used for disaster recovery, Parallel Sysplex combines data sharing and parallel computing to allow a cluster of up to 32 systems to share a workload for high performance and high availability.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: CDCO Supported Architecture Components

Vendor Name: IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	866: Dependent Platform

Operating Systems Supported

- z/OS

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Oracle RAC

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	See z/OS for release and VA Forecast information

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.189) Password Services

General Information

Description: A password is a protected and private string of numbers, text, and other characters used to authenticate an identity.

A password is an un-spaced sequence of characters used to determine that a computer user requesting access to a computer system is really that particular user. Typically, users of a multi-user or securely protected single-user system claim a unique name (often called a userID) that can be generally known. In order to authenticate that someone entering that user ID really is that person, a second identification, the password, known only to that person and to the system itself, is entered by the user.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Password Management Policy		VA Information System Account and Password Management Policy (January 2000)

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
NSA - Network Security Guide	The 60 Minute Network Security Guide
NIST FIPS 48	Guidelines On Evaluation Of Techniques For Automated Personal Identification
NIST FIPS 112	Password Usage
NIST FIPS 181	Automated Password Generator (APG)
NIST FIPS 190	Guideline For The Use Of Advanced Authentication Technology Alternatives
NIST SP 800-12	An Introduction to Computer Security: The NIST Handbook
NIST SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
NIST SP 800-23	Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.190) Performance Management

General Information

Description: Performance management measures available performance parameters to ensure that acceptable levels of performance are maintained. Performance management strives to achieve network conditions where users are satisfied in terms of network responsiveness. Performance management evaluates and reports on the behavior of telecommunications equipment and the effectiveness of the network or network devices. End-to-end performance management measures performance across an internetwork. Component performance measures the performance of individual links or devices. Performance management gathers statistical information, maintains and examines historical logs, determines system performance under natural and simulated conditions.To ensure that the VA is receiving a maximum return on its technical investment, service level agreements (SLAs) should be obtained to confirm that the performance is at the expected levels.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Network Management		The network management system shall display management data, monitor and control managed devices, and communicate with management agents. Data link and physical layer parameters shall be monitored by management systems that are based on Management Information Base (MIB) - Remote Monitoring (RMON) standards.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description

Management Device	A router, server, switch, or end system should be selected on each network to be a local management device.
Problem Notification	Users should be informed about ongoing problems, and given a timeframe for resolution.
Problem Resolution Documentation	After a problem is resolved, the problem/resolution should be tested and then documented in a problem-tracking database.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	Network Management Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.191) Pharmacological Orders Exchange

General Information

Description:	Pharmacological Orders Exchange standards allow pharmacies to standardize information between health care providers and the pharmacies for ordering drugs and to facilitate electronic submission of pharmacy claims at the point of service.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.192) PlateSpin Migrate

General Information

Website: http://www.novell.com/products/migrate/

Description: PlateSpin Migrate is a workload portability solution that automates the movement of server workloads - operating systems along with their applications and data - over the network between physical

servers, virtual hosts and image archives. PlateSpin Migrate remotely decouples workloads from the underlying server hardware and streams them to and from physical or virtual hosts, all from a single point of control.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: CDCO Supported Architecture Components

Vendor Name: Novell

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	Network Management Services*

Operating Systems Supported

- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
8.1	7/24/2008		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
8.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.193) PlateSpin PowerConvert

General Information

Website: http://www.platespin.com/products/powerconvert/

Description: PowerConvert is a workload portability and protection solution that optimizes the data center by streaming server workloads over the network between physical servers, virtual hosts and image archives. PowerConvert remotely decouples workloads from the underlying server hardware and streams them to and from any physical or virtual host.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: CDCO Supported Architecture Components

Vendor Name: Novell

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	Network Management Services*

Operating Systems Supported

- Red Hat Linux
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Internet Information Services (IIS) - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
6.6	5/15/2007		
7.0	6/24/2008		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
7.0	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.194) PlateSpin Protect

General Information

Website:	http://www.novell.com/products/protect/
Description:	PlateSpin Protect is a workload protection solution that replicates and rapidly recovers server workloads - operating systems along with their applications and data - all from a single point of control. In the event of a production server outage or disaster, workloads can be rapidly powered on and continue to run as normal until the production environment is restored. PlateSpin Protect provides a simple, flexible and cost-effective solution for protecting physical and virtual workloads in the data center.
Decision:	Approved
Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	Novell

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	Network Management Services*

Operating Systems Supported

- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
8.0	12/6/2008		
8.1	7/25/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009	CY2010	CY2011

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
8.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.195) Point-to-Point Protocol (PPP)

General Information

Website: http://tools.ietf.org/html/rfc2153

Description: Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. PPP defines an extensible Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection; and a family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2153	5/1/1997		
RFC 5342	9/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is

considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2153	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.196) Portable Document Format (PDF)

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51502

Description: ISO 32000-1: Portable Document Format (PDF) specifies a digital form for representing electronic documents to enable users to exchange and view electronic documents independent of the environment in which they were created or the environment in which they are viewed or printed.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	Native Document Formats*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Rich Text Format (RTF)
- Office Open XML

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2008 (aka PDF 1.7)	7/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2008 (aka PDF 1.7)	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.197) Portable Network Graphics (PNG)

General Information

Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=29581

Description: Portable Network Graphics (PNG, pronounced "ping") specifies a datastream and an associated file format, for a lossless, portable, compressed individual computer graphics image transmitted across the Internet. Indexed-colour, greyscale, and truecolour images are supported, with optional transparency. Sample depths range from 1 to 16 bits. PNG is fully streamable with a progressive display option.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2003	11/10/2003		
2004	3/3/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2004	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.198) Portlet

General Information

Website: http://www.jcp.org/en/jsr/all

Description: To enable interoperability between Portlets and Portals, this specification defines a set of APIs for Portal computing addressing the areas of aggregation, personalization, presentation and security.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	Sun Microsystems

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Portlet specification 1.0	
Portlet specification 2.0	
Portlet Bridge Specification for JavaServer Faces	The Portlet Bridge Specification for JavaServer Faces defines the semantics of a JSR 168/JSR 286 portlet that proxies for JSF artifacts.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	10/27/2003		
2.0	6/12/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.199) Post Office Protocol (POP)

General Information

Website: http://tools.ietf.org/html/rfc2449

Description: Post Office Protocol (POP) is an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2449	11/1/1998		
RFC 5034	7/1/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2449	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.200) PPP Triple-DES Encryption Protocol (3DESE)

General Information

Website: http://www.rfc-editor.org/rfcsearch.html

Description: The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links.

The PPP Encryption Control Protocol (ECP) provides a method to negotiate and utilize encryption protocols over PPP encapsulated links.

This document provides specific details for the use of the Triple-DES standard (3DES) for encrypting PPP encapsulated packets.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2420	9/1/1998		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2420	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.201) Processor Area Network (PAN) Manager

General Information

Website:	http://www.egenera.com/products-panmanager-ex.htm
Description:	Processor Area Network (PAN) Manager aggregates and abstracts industry-standard x86 servers, I/O, SAN storage and data networks into agile resource pools, enabling those resources to be rapidly and automatically re-allocated based upon business requirements.
Decision:	Approved
Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	Egenera

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5.2	1/20/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009	CY2010	CY2011

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
5.2	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.202) Protected Extensible Authentication Protocol (PEAP)

General Information

Website: http://googleads.sgdoubleclick.net/pagead/nclk?sa=L&ai=1&fadurl=googleads.g.doubleclick.net&u=http%3A%2F%2Fdownload.microsoft.com%2Fdownload%2F9%2F5%2FE%2F95EF66AF-9026-4BB0-A41D-A4F81802D92C%2F%255BMS-PEAP%255D.pdf&aclck=http%3A%2F%2Fbabythought.com%2Findex.php

Description: Protected Extensible Authentication Protocol (PEAP) is a part of the family of Extensible Authentication Protocol (EAP) protocols. PEAP uses Transport Level Security (TLS) to create an encrypted channel between an authenticating PEAP client, such as a wireless computer, and a PEAP authenticator, such as an Internet Authentication Service (IAS) or Remote Authentication Dial-In User Service (RADIUS) server. PEAP does not specify an authentication method, but provides additional security for other EAP authentication protocols, such as EAP-MSCHAPv2, that can operate through the TLS encrypted channel provided by PEAP. PEAP is used as an authentication method for 802.11 wireless client computers, but is not supported for virtual private network (VPN) or other remote access clients.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision TRMSP 4.3.2

Process:
Decision Date: 3/14/2008
Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: Microsoft

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Transport Layer Security (TLS) Protocol - Standard
- Remote Authentication Dial In User Service (RADIUS) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
v0/EAP-MSCHAPv2			
v1/EAP-GTC			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
v0/EAP-MSCHAPv2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.203) Public Key Infrastructure

General Information

Description: The Public Key Infrastructure (PKI) is a framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies.

PKI provides for a digital certificate that can identify an individual or

an organization and directory services that canstore and, when necessary, revoke the certificates. PKI facilitates the use of public key cryptography, which is acommon method for authenticating an individual or encrypting a file. PKI consists of:

- A certificate authority (CA) issues and verifies digital certificate. A certificate includes the public key orinformation about the public key
- A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate isissued to a requestor
- One or more directories where the certificates (with their public keys) are held
- A certificate management system

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Federal Bridge Certificate Authority (FBCA) Certificate Policy		X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)
VA PKI Certificate Policy		Department of Veterans Affairs, VA PKI: Certificate Policy, DRAFT v2.0, June 14, 1999

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
NIST FIPS 48	Guidelines On Evaluation Of Techniques For Automated Personal Identification
NIST FIPS 190	Guideline For The Use Of Advanced Authentication Technology Alternatives

NIST FIPS 196	Entity Authentication Using Public Key Cryptography
NIST SP 800-2	Public-Key Cryptography
NIST SP 800-15	Minimum Interoperability Specification for PKI Components (MISPC), Version 1
NIST SP 800-21	Guideline for Implementing Cryptography in the Federal Government
NIST SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
NIST SP 800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure
IETF RFC 3447	PKCS #1-RSA Cryptography Standard: RSA Cryptography Specifications V2.1
IETF RFC 2315	PKCS #7-Cryptographic Message Syntax v1.5
IETF RFC 2527	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
IETF RFC 2631	PKCS #3-Diffie-Hellman Key Agreement Method
IETF RFC 2985	PKCS #9-Selected Object Classes and Attribute Types v2.0
IETF RFC 2986	PKCS #10-Certification Request Syntax Specificatio v1.7
PKCS #6	PKCS #6-Extended-Certificate Syntax Standard
PKCS #8	PKCS #8-Private-Key Information Syntax Standard
PKCS #11	PKCS #11-Cryptographic Token Interface Standard
PKCS #12	PKCS #12-Personal Information Exchange Syntax Standard
PKCS #13	PKCS #13-Elliptic Curve Cryptography Standard
ASTM E2212-02	Standard Practice for Healthcare Certificate Policy

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.204) Pulse Code Modulation (PCM) of Voice Frequencies

General Information

Website:	http://www.itu.int/itu-t/recommendations/index.aspx?ser=G
Description:	ITU-T G.711: Pulse Code Modulation (PCM) of Voice Frequencies defines the characteristics for encoding voice-frequency signals.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5	11/15/1988		
5.1	9/30/1999		
5.2	2/12/2000		
5.3	8/29/2009		
5.4	11/6/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
5.2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.205) Radio Frequency Management

General Information

Description:	Radio Frequency (RF) services provide the capability for all radio communication devices to transmit and receive efficiently. Radio communication devices in a given area must cooperate if they are to avoid interference problems. If they operate on the same frequencies, at the same time and in the same area, their transmissions produce interference in each other's receivers. RF services regulate the spectrum and controls access because of the potential for interference between uncoordinated uses. Frequency management provides guidance and support for the assignment, management, and use of radio frequencies used by all elements of the VA. The most common use for VA frequency management is mobile communications, using Ultra High Frequency (UHF) and Very High Frequency (VHF). As the demand for frequency usage has increased, technology has developed radios that can perform the same function at higher unused frequencies or with decreased bandwidth at the same frequency. The VA is converting wideband 25-kilohertz (kHz) channels to narrowband 12.5 kHz channels. The conversion doubles the number of channels and provides communications capability for more users.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Approval		The use and acquisition of all VA telecommunications radio equipment shall be approved by the National Telecommunications and Information Administration (NTIA) Interdepartmental Radio Advisory Committee.
Assignment Duration		Radio frequency assignments shall be valid for five years.

Guidelines and Best Practices

No guidelines have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	Network Management Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.206) Rational ClearCase with MultiSite

General Information

Website: http://www-306.ibm.com/software/awdtools/clearcase/

Description: Rational ClearCase is a software configuration management solution that provides version control, workspace management, and build auditing. ClearCase supports parallel development and, coupled

with MultiSite, geographically distributed development.

Decision: Approved

Decision Constraints: Contact the Software Engineering Tools Management Division for details on the constraints for use of this technology.

Decision Source: ARB

Decision Process: TRM v2

Decision Date: 9/17/2008

Current Status: Analysis Completed

Introduced By: Extended Tool List (ETL)

Vendor Name: IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	868: Software Configuration Management

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

- Eclipse - ***(required for some configurations)***

Comparable Technologies/Standards:

- Rational Team Concert

Companion Technologies/Standards:

- Rational ClearQuest with MultiSite related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2003.06	10/1/2003	9/30/2008	
7.0.0.0	6/6/2006		
7.0.1.0	7/1/2007		
7.0.2 (est)	4/1/2009		
7.0.3 (est)	4/1/2010		
8.0 (est)	9/30/2010		

VA Forecast Information (09/25/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2008				CY2009				CY2010			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2003.06	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
7.0.0.0	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**
7.0.	No	No	No	No	No	No	No	No	**Planni**	**Evalu**	**Supp**	**Supp**

2 (est)	ne	ne	ne	ne	ne	ne	ne	ne	ng	ation	orted	orted
Forecast Note:												

General Analysis

Architectural Area

- Application

Architectural Benefits

- The deployment and use of a standard software configuration management solution provides a common toolset which leads to improvements in efficiency.

Architectural Risks

- The ClearCase solution has a relatively high learning curve and requires significant management overhead in terms of computing resources and personnel.

Tier Used

- Infrastructure Tier

Tool Type

- Tool

Tool Usage

- Management/Collaboration
- Development

General Assessment

Expected Usage:	ClearCase is a software configuration management tool to manage code baselines providing version control, build and workspace management, and parallel development support.
Assessment Type:	Refresh
Assessment Date:	9/25/2008
Notes:	
Recommendation:	Approve

Recommendation Constraints:	
Recommendation Justification:	A standardized software configuration management solution provides a consistent approach to develop and deliver HeV solutions.

4.207) Rational Software Modeler

General Information

Website:	http://www-01.ibm.com/software/awdtools/modeler/swmodeler/index.html
Description:	Rational Software Modeler (RSM) is a UML 2.0 based modeling and design tool. Built on top of the Eclipse platform, this product offers a plethora of UML modeling and software design-construction functionality. RSM contains a subset of Rational Software Architect.
Decision:	Approved
Decision Constraints:	Contact the Software Engineering Tools Management Division for details on the constraints for use of this technology.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Introduced
Introduced By:	Enterprise Tools Management
Vendor Name:	IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code

Service Platform and Infrastructure	Software Engineering	867: Integrated Development Environments (IDE)

Operating Systems Supported

- Red Hat Linux
- Windows (Client)

Technologies/Standards Relationships

Runtime Dependencies:

- Eclipse - ***(required libraries)***
- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- Rational Rose

Companion Technologies/Standards:

- Rational Software Architect related as: (Companion)
- Rational Systems Developer related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
7.0	12/5/2006		
7.0.0.2	4/9/2007		
7.0.0.4	9/28/2007		
7.0.5.0	12/14/2007		
7.0.5.1	3/27/2008		
7.0.5.2	6/26/2008		
7.0.5.3	12/11/2008		
7.5	10/1/2008		
7.5.1	12/11/2008		
8.0 (est)	9/30/2009		

VA Forecast Information (10/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
7.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
7.0.5.0	None	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
7.5	None	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. The Benefits Segment use of Software Modeler is currently based on version 7.5.

General Analysis

Architectural Area

- Application

Architectural Benefits

- Support for HTML, DHTML, XHTML, CHTML, JavaScript, CSS
- Support for building J2EE applications
- Deploy J2EE applications to WebLogic server
- Support for JAR, EAR, WAR packaging

Architectural Risks

- Potential for vendor lock-in
- Better integration with IBM WebSphere than WebLogic

EA Requirement

- ENTR 1074 - Implement a One VA information technology framework that supports the integration of information across business lines and that provides a source of

consistent, reliable, accurate, and secure information to veterans and their families, employees, and stakeholders (Enabling Objective E-3).

Standards Traceability

- EJB 1.1, 2.0, 2.1
- JAXP 1.2 (J2EE 1.4), 1.3 (J2SE 5)
- SOAP 1.1, 1.2
- JNDI 1.2.1
- JSP 1.1, 1.2, 2.0
- J2EE 1.2, 1.3, 1.4
- JDBC 3.0
- Servlet 2.3, 2.4

Tier Used

- Other Tier

Tool Type

- Commercial

Tool Usage

- Development

General Assessment

Expected Usage:	IDE
Assessment Type:	Refresh
Assessment Date:	2/12/2009
Notes:	Rational Software Modeler contains a subset of functionality of Rational Software Architect, as do other Rational modeling tools such as Systems Developer and Application Developer.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Rational Software Modeler is in the current baseline of tools offered by the OED Tools Management Division.

4.208) Regulations and Procedures for Federal Radio Frequency Management

General Information

Website:	http://www.ntia.doc.gov/osmhome/redbook/redbook.html
Description:	Regulations and Procedures for Federal Radio Frequency Management is the official source for all technical regulations relating to the use of the electromagnetic frequency spectrum.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	NTIA

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2008	1/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2008	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.209) Remote Access Protocol

General Information

Description: Remote Access services enable users at remote locations to connect to enterprise network services and applications from almost anywhere. Remote access provides contact from telecommuter sites, mobile computing, as well as technical support. Atelecommuter site is a small office with one to a few employees. It can also be atelecommuter's home office. Telecommuters can also refer to mobile users whotravel. Mobile computing allows field representatives to access office resources onthe road. Technical support can dial in to client systems to diagnose and correctproblems remotely. One difference between a remote host and local-basedworkstations connected directly to the network is slower data transfer speeds. Userscan access the network via a Virtual Private Network (VPN) or traditional dial-up.VPNs allow users and customer's access to the VA network while providing asecure connection. Private data is encrypted for routing through the serviceprovider's network or the Internet.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Dialup		Point-to-point protocol (PPP) shall be used as the

		transporting network layer protocol across dialup serial point-to-point links.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
High Speed Access	Users who want higher speeds than analog can establish remote access with cable modems, DSL, or a router that has access to a WAN port.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.210) Remote Authentication Dial In User Service (RADIUS)

General Information

Website: http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

Description: Remote Authentication Dial In User Service (RADIUS) is a protocol for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server.

Decision: Approved

Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2865	6/1/2000		
RFC 3575	7/1/2003		
RFC 5080	12/1/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2865	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.211) Rich Text Format (RTF)

General Information

Website: http://www.microsoft.com/downloads/details.aspx?familyid=DD422B8D-FF06-4207-B476-6B5396A18A2B&displaylang=en

Description:	The Rich Text Format (RTF) specification provides a format for text and graphics interchange that can be used with different output devices, operating environments, and operating systems.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	Microsoft

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	Native Document Formats*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Portable Document Format (PDF)
- Office Open XML

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.8	4/1/2004		
1.9.1	3/20/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.8	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.9.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.212) Scalable Vector Graphics (SVG)

General Information

Website:	http://www.w3.org/TR/SVG11/
Description:	Scalable Vector Graphics (SVG) is a family of specifications of an XML-based file format for describing two-dimensional vector graphics, both static and dynamic (i.e. interactive or animated).
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.1	1/14/2003		
1.2 (Tiny)	12/22/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
1.2 (Tiny)	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.213) Secure Code Design

General Information

Description: Secure code design is a set of engineering principles for designing system security. These principles provide a foundation upon which a more consistent and structured approach to the design, development, and implementation of IT security capabilities can be constructed. While the primary focus of these principles is the implementation of technical controls, these principles highlight the fact that, to be effective, a system security design should also consider non-technical issues, such as policy, operational procedures, and user education.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
NIST SP 800-27	Engineering Principles for Information Technology Security (EP-ITS) presents a list of system-level security principles to be considered in the design, development, and operation of an information system.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Security Controls*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.214) Secure Hash Standard (SHS)

General Information

Website:	http://csrc.nist.gov/publications/PubsFIPS.html
Description:	FIPS 180: This standard specifies five hash algorithms that can be used to generate digests of messages. The digests are used to detect whether messages have been changed since the digests were generated.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	NIST

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2	8/1/2002		
3	10/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or

production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.215) Secure Hypertext Transfer Protocol (S-HTTP)

General Information

Website: http://www.rfc-editor.org/rfcsearch.html

Description: Secure Hypertext Transfer Protocol (S-HTTP) is a protocol for securing messages sent using the Hypertext Transfer Protocol (HTTP), which forms the basis for the World Wide Web. Secure HTTP (S-HTTP) provides independently applicable security services for transaction confidentiality, authenticity/integrity and non-repudiability of origin.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2660	8/1/1999		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on

the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2660	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.216) Secure Remote Access with L2TP

General Information

Website: http://tools.ietf.org/html/rfc2888

Description: Secure Remote Access with L2TP extends the security characteristics of IPsec to remote access users, as they dial-in through the Internet.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Remote Authentication Dial In User Service (RADIUS) - Standard
- Point-to-Point Protocol (PPP) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2888	8/1/2000		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2888	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.217) Secure/Multipurpose Internet Mail Extensions (S/MIME) Certificate Handling

General Information

Website: http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

Description: Secure/Multipurpose Internet Mail Extensions (S/MIME) Certificate Handling provides a method to send and receive secure MIME messages.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2632	6/1/1999		
RFC 3580	7/1/2004		

RFC 5750	1/1/2010		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
RFC 2632	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.218) Secure/Multipurpose Internet Mail Extensions (S/MIME) Message Spec

General Information

Website: http://www.rfc-editor.org/rfcsearch.html

Description: Secure/Multipurpose Internet Mail Extensions (S/MIME) provides a consistent way to send and receive secure MIME data. Based on the popular Internet MIME standard, S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption).

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.0 (RFC 2633)	6/1/1999		
3.1 (RFC 3851)	7/1/2004		
3.2 (RFC 5751)	1/1/2010		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.219) Securing Layer Two Tunneling Protocol (L2TP) with IPsec

General Information

Website: http://tools.ietf.org/html/rfc3193

Description: Securing Layer Two Tunneling Protocol (L2TP) with IPsec discusses how L2TP may utilize IPsec to provide for tunnel authentication, privacy protection, integrity checking and replay protection.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3193	11/1/2001		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 3193	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.220) Security Architecture for the Internet Protocol (IP)

General Information

Website: http://tools.ietf.org/html/rfc4301

Description: Security Architecture for the Internet Protocol (IP) describes the security mechanisms for IP version 4 (IPv4) and IP version 6 (IPv6) and the services that they provide. This document also describes key management requirements for systems implementing those security mechanisms.

Decision: Approved

Decision No constraints have been specified at this time.

Constraints:

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 1825	8/1/1995	11/1/1998	
RFC 2401	11/1/1998	12/1/2005	
RFC 4301	12/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 4301	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.221) Security Architecture for the Internet Protocol (IPSec)

General Information

Website: http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

Description: Security Architecture for the Internet Protocol (IPSec) specifies the base architecture for IPSec compliant systems. The goal of the architecture is to provide various security services for traffic at the IP

layer, in both the IPv4 and IPv6 environments.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2401	11/1/1999		
RFC 4301	12/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2401	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.222) Security Assertion Markup Language (SAML)

General Information

Website: http://www.oasis-open.org/specs/#samlv2.0

Description: The Security Assertion Markup Language (SAML) specification

	defines the syntax and semantics for XML-encoded assertions about authentication, attributes, and authorization, and for the protocols that convey this information.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	Benefits Arch
Decision Process:	TRM v4.1
Decision Date:	10/28/2009
Current Status:	Analysis Completed
Introduced By:	Benefits ASA
Vendor Name:	OASIS

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Requirements	860: Authentication / Single Sign-on

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- WS-Security - Standard
- Extensible Markup Language (XML) - Standard
- XML Namespaces (XML-NS) - Standard
- XML Schema - Standard
- Simple Object Access Protocol (SOAP) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	11/1/2002		
1.1	8/28/2003		
2.0	2/28/2005		

VA Forecast Information (10/09/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2.0	None	None	None	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Adoption Benefits

- SAML is mature and a widely adopted industry standard.

Architectural Benefits

- SAML defines a federated identities approach that insures identities are both portable and potable, that is, they can be transported and consumed across autonomous domains or business boundaries.
- SAML is platform independent. The security framework is abstracted away from platform architectures and particular vendor implementations. Making security more independent of application logic is an important tenet of Service-Oriented Architecture.
- SAML is loose coupling of directories. User information is not required to be maintained and synchronized between directories.
- SAML defines a single sign-on approach, allowing users to authenticate at an identity provider and then access service providers without additional authentication.

General Assessment

Expected Usage:	Specification for service authentication, authorization, and single sign-on.
Assessment Type:	New
Assessment Date:	11/4/2009
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	SAML is a mature, widely adopted industry standard for federated identity. It defines standardized mechanisms for the communication of security and identity information.

4.223) Security Requirements for Cryptographic Modules

General Information

Website:	http://csrc.nist.gov/publications/PubsFIPS.html
Description:	FIPS 140: Security Requirements for Cryptographic Modules specifies the security requirements that will be satisfied by a cryptographic module. The standard provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security;

operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: NIST

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2	5/1/2001		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.224) Security Token

General Information

Description:	A Security Token is a physical device, such as a special smart card, that together with something that a user knows, such as a PIN, enables authorized access to a computer system or network.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
NIST FIPS 190	Guideline For The Use Of Advanced Authentication Technology Alternatives
NIST FIPS 196	Entity Authentication Using Public Key Cryptography
NIST SP 500-157	Smart Card Technology: New Methods for Computer Access Control
NIST IR 6887	Government Smart Card Interoperability Specification
PKCS #11	Cryptographic Token Interface Standard
PKCS #15	Cryptographic Token Information Format Standard
ISO/IEC 7816-4	Organization, security and commands for interchange

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.225) Servers

General Information

Refer to document:	VA_Enterprise_Server_Standards_1_0.pdf
Description:	This standards document lists the acceptable and recommended specifications for Server Platforms. Sections include standard specifications for subject components, decisions supporting the standard specifications, guidelines or recommendations for implementing the standard specifications, and supplemental factors to consider for when evaluating subject components. Other supplementary documents will provide guidance on procuring components that meet the standard specifications, guidance on integrating them with existing components, and explanation of how the subject components fit into the VA Architecture. This standard includes the following: Light Workload Server (Class C); Typical Workload Server (Class B); Heavy Workload Server (Class A); VistA Back-End Server (Class E). For each of these standards the following supporting details are included; Processor; Performance; Memory; Internal Storage; External Storage Interface; Server Communications Interface; Removable Media Device; Power; Cooling Fan.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision	EIE CTO

Source:	
Decision Process:	TAR-TAS
Decision Date:	11/18/2009
Current Status:	Analysis Completed
Introduced By:	OPS/EIE

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	877: Servers / Computers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.226) SharePoint Server

General Information

Website: http://sharepoint.microsoft.com/Pages/Default.aspx

Description: SharePoint Server, also known as Microsoft Office SharePoint Server (MOSS), is a content management system with integrated search functionality that allows users to work in a web-based collaborative environment.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	Microsoft

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Access Channels	852: Collaboration / Communications

Operating Systems Supported

- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- SQL Server - ***(required libraries)***

Comparable Technologies/Standards:

- TeamPage
- TWiki
- MediaWiki

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2003	10/21/2003		
2003 SP1	10/18/2004		
2003 SP2	10/18/2005		
2003 SP3	9/17/2007		
2007	11/7/2006		
2007 SP1	12/8/2007		
2007 SP2	7/29/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2007 SP1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.227) Simple Mail Transfer Protocol (SMTP)

General Information

Website: http://tools.ietf.org/html/rfc2821

Description:	Simple Mail Transfer Protocol (SMTP) is a specification of the basic protocol for the Internet electronic mail transport.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
SMTP Service Extension for Returning Enhanced Error Codes	This document defines an extension to the SMTP service whereby an SMTP server augments its responses with the enhanced mail system status codes.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2821	4/1/2001		
RFC 5336	9/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2821	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.228) Simple Network Management Protocol (SNMP)

General Information

Website: http://tools.ietf.org/html/rfc3412

Description: Simple Network Management Protocol (SNMP) describes the Message Processing and Dispatching for SNMP messages within the SNMP architecture. It defines the procedures for dispatching potentially multiple versions of SNMP messages to the proper SNMP Message Processing Models, and for dispatching Protocol Data Units (PDUs) to SNMP applications.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- User Datagram Protocol (UDP) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3412	12/1/2002		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 3412	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.229) Simple Object Access Protocol (SOAP)

General Information

Website:	http://www.w3.org/TR/
Description:	Simple Object Access Protocol (SOAP) is a lightweight protocol intended for exchanging structured information in a decentralized, distributed environment. SOAP is fundamentally a stateless, one-way message exchange paradigm, but applications can create more complex interaction patterns (e.g., request/response, request/multiple responses, etc.) by combining such one-way exchanges with features provided by an underlying protocol and/or application-specific information. SOAP is silent on the semantics of any application-specific data it conveys, as it is on issues such as the routing of SOAP messages, reliable data transfer, firewall traversal, etc. However, SOAP provides the framework by which application-specific information may be conveyed in an extensible manner. Also, SOAP provides a full description of the required actions taken by a SOAP node on receiving a SOAP message.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	Benefits Arch
Decision Process:	TRM v4.1
Decision Date:	10/28/2009
Current Status:	Analysis Completed
Introduced By:	Benefits ASA
Vendor Name:	W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Transport	HTTP is the preferred SOAP transport protocol.
Fault Codes	SOAP Fault Codes are the preferred method for handling problems since throwing exceptions canonly be successfully caught if the “client” is also using Java.

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Primer	Primer is a non-normative document intended to provide an easily understandable tutorial on the features of SOAP. In particular, it describes the features through various usage scenarios, and is intended to complement the normative text contained in Part 1 and Part 2 of the SOAP specifications.
Messaging Framework	Messaging Framework defines, using XML technologies, an extensible messaging framework containing a message construct that can be exchanged over a variety of underlying protocols.
Adjunts	Adjuncts defines a set of adjuncts that may be used with SOAP Messaging Framework.
Assertions and Test Collection	This document draws on assertions found in the SOAP specifications and provides a set of tests in order to show whether the assertions are implemented in a SOAP processor.
SOAP Message Transmission Optimization Mechanism (MTOM)	This document describes an abstract feature and a concrete implementation of it for optimizing the transmission and/or wire format of SOAP messages.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Extensible Markup Language (XML) - Standard
- XML-Infoset - Standard
- XML Schema - Standard
- XML Namespaces (XML-NS) - Standard
- Security Assertion Markup Language (SAML) - Standard
- WS-I Basic Profile - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.1	5/8/2000		
1.2	4/27/2007		

VA Forecast Information (09/28/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.2	None	None	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Architectural Benefits

- Interoperability - platform independent
- Interoperability - supports multiple transport protocols (HTTP and SMTP)
- SOAP over HTTP allows for easier communication through proxies and firewalls than other remote execution technologies
- Extensible - (WS-Security is an SOAP extension)

Tier Used

- Middle Tier (Integration)

General Assessment

Expected Usage:	A standard for exchanging XML based messages over HTTP
Assessment Type:	Standard
Assessment Date:	11/3/2009
Notes:	HTTP is the preferred SOAP transport protocol since it can be more easily secured using SSL.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	SOAP is a mature, widely adopted industry standard. It is a highly interoperable messaging specification. SOAP provides a more secure approach than REST as sensitive data should not be sent as parameters in URIs.

4.230) Single Sign On

General Information

Description:	Single Sign On (SSO) is a session or user authentication process that permits a user to enter one name and password in order to access multiple applications. The SSO, whichis requested at the initiation of the session, authenticates the user to access all the applications and data to which they have rights on the system, and eliminates future authentication prompts when the user switches applications during that particular session.

Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
NIST FIPS 48	Guidelines On Evaluation Of Techniques For Automated Personal Identification
NIST SP 800-23	Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.231) Solaris

General Information

Website:	http://www.sun.com/software/solaris
Description:	The Solaris Operating System (OS) is a free and open UNIX operating system. It is available for both x86 and SPARC systems. The vendor (Sun) supports the development of Solaris via the OpenSolaris project, an open source community and a place for collaboration and conversation around Solaris technology. In June 2005, Sun initiated the project by releasing the source code for the core kernel, libraries and commands of the Solaris Operating System under the terms of the OSI-approved Common Development and Distribution License (CDDL).
Decision:	Approved
Decision Constraints:	Products that have been deployed to a production environment may continue to use this technology. All other products must utilize a One-VA TRM approved Linux operating system.
Decision Source:	ARB
Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	TRM Team
Vendor Name:	Sun Microsystems

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	866: Dependent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Red Hat Linux
- AIX
- HP-UX
- Windows (Server)

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
9 9/05	9/1/2005	4/28/2009	10/30/2014
10 1/06	1/1/2006		
10 6/06	6/1/2006		
10 11/06	11/1/2006		
10 8/07	8/1/2007		
10 5/08	5/1/2008		
10 10/08	10/31/2008		
10 5/09	5/1/2009		

VA Forecast Information (04/09/2010)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on

the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
9 9/05	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
10 6/06	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
10 11/06	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
10 8/07	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
10 10/08	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Architectural Benefits

- Solaris support for both Sun proprietary and x86 hardware greatly enhances interoperability, operations, security, and utilization of physical layer components.

Architectural Risks

- Specialized, proprietary expertise is required to build-maintain Solaris servers.

Tier Used

- Data Tier
- Middle Tier (Infrastructure)
- Middle Tier (Business)
- Middle Tier (Integration)

Tool Type

- Platform

Tool Usage

- Development
- Runtime

General Assessment

Expected Usage:	The inclusion of Solaris into the TRM fulfills the objectives outlined in ENTR68 (now marked as inactive).
Assessment Type:	Refresh
Assessment Date:	9/23/2008
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Recommend approval as Solaris is successfully implemented in the HeV infrastructure without issue.

4.232) Stateless Dynamic Host Configuration Protocol (DHCPv6)

General Information

Website:	http://tools.ietf.org/html/rfc3736
Description:	Stateless Dynamic Host Configuration Protocol service for IPv6 (DHCPv6) is used by nodes to obtain configuration information, such as the addresses of DNS recursive name servers, that does not require the maintenance of any dynamic state for individual clients. A node that uses stateless DHCP must have obtained its IPv6 addresses through some other mechanism, typically stateless address autoconfiguration.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA

Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3736	4/1/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 3736	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.233) Static Display

General Information

Description: Static Display consists of the software protocols that are used to create a predefined, unchanging graphical interface between the user and the software.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Styles	When possible, use an externally linked, single style sheet (CSS) for an entire site to help enforce a consistent look and feel.
Organization	The preferred method of organizing files numbering over a few dozen is to have the directory structure mirror the major navigation of a site with graphics in a separate (images) subdirectory.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	886: Static Display

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.234) Storage

General Information

Refer to document:	VA_Enterprise_Storage_Standard_1_0.pdf
Description:	This standards document lists the acceptable and recommended specifications for general and mission critical backend storage devices, storage area network, and backup solution. Sections include standard specifications for subject components, decisions supporting the standard specifications, guidelines or recommendations for implementing the standard specifications, and supplemental factors to consider when evaluating subject components. Other supplementary documents will provide guidance on procuring components that meet the standard specifications, guidance on integrating them with existing components, and explanation of how the subject components fit into the VA Architecture. This standard includes the following: Tier 1 Storage Service; Tier 2 Storage Service; Tier 3 Storage Service; General Storage Area Network; General Backup and Archive. For each of these standards, the following supporting details are included per tier, as appropriate; Storage Subsystem Hardware; Storage Management Software; Hardware/Software Technical Support; Hardware/Software Installation; Training; LAN Connectivity; Fabric Switch Hardware; SAN Management Software; Backup Method; Virtual Tape Library Hardware; Archive Hardware; Tape Library Hardware; Backup Software/VTL/Archive/Tape Library Tool.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EIE CTO
Decision Process:	TAR-TAS
Decision Date:	11/18/2009
Current Status:	Analysis Completed
Introduced By:	OPS/EIE

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Database/Storage	876: Storage Devices

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be

supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.235) Strobe

General Information

Website: http://www.compuware.com/solutions/strobe.asp

Description: Strobe measures mainframe application performance of both online and batch-processing applications while identifying chronic, recurring application failures that consume Central Processor Unit (CPU) utilization.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: CDCO Supported Architecture Components

Vendor Name: Compuware

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	Network Management Services*

Operating Systems Supported

- z/OS

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- BMC Mainview

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.0	4/8/2003		
3.2	3/23/2005		
4.1	2/2/2010		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on

the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
3.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.236) Structured Query Language (SQL)

General Information

Website: http://webstore.ansi.org/RecordDetail.aspx?sku=INCITS%2fISO%2fIEC+9075-1-2003

Description: Structured Query Language (SQL) is a database computer language designed for managing and querying data in a relational database management systems (RDBMS).

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: Benefits Arch

Decision Process: TRM v4.1

Decision Date: 10/28/2009

Current Status: Analysis Completed

Introduced By: Benefits ASA

Vendor Name: ANSI

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Framework (SQL/Framework)	ISO/IEC 9075-1 specifies the conceptual framework used in other parts of ISO/IEC 9075 to specify the grammar of SQL and the result of processing statements in that language by an SQL-implementation.
Foundation (SQL/Foundation)	ISO/IEC 9075-2 defines the data structures and basic operations on SQL-data. It provides functional capabilities for creating, accessing, maintaining, controlling, and protecting SQL-data. Both static and dynamic variants of the language are proved. In addition to direct invocation, bindings are provided for the programming languages Ada, C, COBOL, Fortran, M, Pascal, and PL/I.
Call-level Interface (SQL/CLI)	ISO/IEC 9075-3 defines the structures and functions that can be used to execute statements of the database language SQL from within an application written in a standard programming language in such a way that the functions used are independent of the SQL statements to be executed.
Persistent Stored Modules (SQL/PSM)	ISO/IEC 9075-4 specifies the syntax and semantics of statements to add a procedural capability to the SQL language in functions and procedures. It includes statements to direct the flow of control, define variables, make assignments and handle exception conditions.
Management of External Data (SQL/MED)	ISO/IEC 9075-9 defines extensions to SQL to support management of external data through the use of foreign-data wrappers and datalink types.
Object Language Bindings (SQL/OLB)	ISO/IEC 9075-10 defines extensions to the SQL language to support embedding of SQL statements into programs written in the Java programming language (Java is a registered trademark of Sun Microsystems, Inc.). In addition it specifies mechanisms to ensure binary portability of resulting applications.
Information and Definition Schemas (SQL/Schemata)	ISO/IEC 9075-11 specifies an Information Schema and a Definition Schema that describe: • the structure and integrity constraints of SQL-data • the security and authorization specifications relating to SQL-datathe security and authorization specifications relating to SQL-data • the features, subfeatures, and packages of ISO/IEC 9075, and the support that each of these has in an SQL implementation

	• the SQL-implementation information and sizing items of ISO/IEC 9075 and the values supported by an SQL-implementation
SQL Routines and Types Using Java (SQL/JRT)	ISO/IEC 9075-13 specifies the ability to invoke static methods written in the Java programming language as SQL-invoked routines and to use classes defined in the Java programming language as SQL structured user-defined types
XML-Related Specifications (SQL/XML)	ISO/IEC 9075-14 defines ways in which Database Language SQL can be used in conjunction with XML.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	895: Middleware

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- XQuery

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
SQL-86			
SQL-89			
SQL-92	7/1/1992		
SQL:1999			
SQL:2003			

SQL:2008	7/17/2008		

VA Forecast Information (10/13/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
SQL:2003	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
SQL:2008	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Adoption Benefits

- Structured Query Language (SQL) is a mature and widely adopted industry standard for managing and querying data in a Relational Database Management Systems (RDBMS).

Adoption Risks

- The Structured Query Language (SQL) does not cover procedural languages, which are the backbone of stored procedures and triggers.
- Though vendors implement the ANSI SQL standards, the version of the standard supported may vary by vendor. Vendors also include product specific language extensions. This may result in vendor lock-in and reduce portability.

Architectural Benefits

- Standardizes the language used to manage and access Relational Database Management Systems (RDBMS).

General Assessment

Expected Will be used as the standard language for managing and querying

Usage:	Relational Database Management Systems (RDBMS).
Assessment Type:	New
Assessment Date:	11/3/2009
Notes:	
Recommendation:	Approve-Conditional
Recommendation Constraints:	Hibernate Query Language (HQL) should be used for RDBMS access with java based components XQuery should be used for XML data access
Recommendation Justification:	SQL is a very mature and widely used industry standard for RDBMS data management.

4.237) Synchronous Optical Network (SONET)

General Information

Website:	http://webstore.ansi.org/RecordDetail.aspx?sku=ATIS-0900105.2008
Description:	ATIS-0900105 (formerly ANSI T1.105): Synchronous Optical Networking (SONET) or Synchronous Digital Hierarchy (SDH) are standardized multiplexing protocols that transfer multiple digital bit streams over optical fiber using lasers or light-emitting diodes (LEDs).
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ANSI

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Digital Hierarchy - Electrical Interfaces	This document defines the contents of the Automatic Protection Switching (APS) bytes within the SONET signal. Formerly known as T1.105.01-2000(R2005).
Jitter Network Interfaces	This document describes the jitter specifications that are applicable to SONET network and equipment interfaces (OC-N and STS-N), and jitter and wander specifications that are applicable to certain SONET payload signals (e.g. DS1 and DS3). Formerly known as T1.105.03-2003(R2008).
Automatic Protection Switching	This document defines the protocols and architectures for data communications using the DCC bytes within the SONET signal. These DCC bytes carry the OAM&P information between network elements and can be used as an integral part of the overall Telecommunications Management Network (TMN). Formerly known as T1.105.04-1995(R2005).
Tandem Connection Maintenance	This document defines the contents and use of the Tandem Connection Monitoring bytes within the SONET signal. Tandem Connection Monitoring provides enhanced maintenance capabilities for certain SONET applications. Formerly known as T1.105.02-2002(R2008).
Physical Layer Specifications	This document provides the necessary parameters for SONET optical links in short reach, intermediate reach, and long reach applications. It also provides references for the necessary parameters in SONET electrical links. Formerly known as T1.105.03-2002(R2007).
Sub STS-1 Interface Rates and Formats Specification	This document defines the formats for the VT1.5 interface and virtual tributary group interface, including the definitions and content of the associated overhead channels. Formerly known as T1.105.07-1996(R2008).
Data Communication Channel Protocol and Architectures	This document defines the SONET overhead byte locations that are used for the error correcting code and the specifications of the code itself. Formerly known as T1.105.08-2001(R2005).
Network Timing and Synchronization	This document provides timing and synchronization specifications for SONET interfaces. Compliance with this standard is necessary to achieve satisfactory interworking of telecommunications networks. Formerly known as T1.105.09-1996(R2008).

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	Metropolitan Area Network (MAN)*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1996	1/1/1996		
2005	1/1/2005		

VA Forecast Information (10/13/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010	CY2011	CY2012

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.238) System for Establishing Communication Between Audiovisual Terminals

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=H

Description: ITU-T H.242: System for Establishing Communication Between Audiovisual Terminals using Digital Channels up to 2 Mbit/s describes all the point-to-point procedures involving the Bit-rate Allocation Signal (BAS) codes: initial capability exchange and mode initialization, including restricted-network operation; in-session mode switching, including audiovisual mode changes and activation of data channels; other procedures, including single/multiple channel interconnection, encryption, mode-preference indication, conveyance of network addresses and use of BAS extension codes.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
6	3/15/2004		
6.1	9/13/2005		
7	3/16/2009		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on

the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
6.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.239) TELNET

General Information

Website: http://tools.ietf.org/html/rfc856

Description: The TELNET Protocol provides a fairly general, bi-directional, eight-bit byte oriented communications facility. Its primary goal is to allow a standard method of interfacing terminal devices and terminal-oriented processes to each other. It is envisioned that the protocol may also be used for terminal-terminal communication ("linking") and process-process communication (distributed computation).

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	871: Web Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 854	5/1/1983		
RFC 855	5/1/1983		

RFC 856	5/1/1983		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
RFC 856	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.240) Temporal Key Integrity Protocol (TKIP)

General Information

Website: https://sbwsweb.ieee.org/ecustomercme_enu/start.swe?SWECmd=GotoView&SWEView=Catalog+View+%28eSales%29_Standards_IEEE&mem_type=Customer&SWEHo=sbwsweb.ieee.org&SWETS=1192713657

Description: Temporal Key Integrity Protocol (TKIP) is a security protocol used in the IEEE 802.11 wireless networking standard.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IEEE

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
802.11-1999			
802.11-2007			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
802.11-1999	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.241) Teredo

General Information

Website: http://msdn.microsoft.com/en-us/library/aa965909%28v=VS.85%29.aspx

Description: Teredo is an IPv6 transition technology that provides address assignment and host-to-host automatic tunneling for unicast IPv6 traffic when IPv6/IPv4 hosts are located behind one or multiple IPv4 network address translators (NATs). To traverse IPv4 NATs, IPv6 packets are sent as IPv4-based User Datagram Protocol (UDP)

messages. This article provides an overview of Teredo - including Teredo addresses and packet structures - and detailed explanations of how communication is initiated between Teredo clients, Teredo host-specific relays, and IPv6-only hosts using the IPv4 Internet, the IPv6 Internet, Teredo servers, and Teredo relays.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: Microsoft

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	See Windows Client and Windows Server for forecast information.

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.242) Transmission of IP Datagrams over SMDS

General Information

Website: http://tools.ietf.org/html/rfc1209

Description:	The Transmission of Internet Protocol (IP) Datagrams over the Switched Multi-megabit Data Service (SMDS) Service describes an initial use of IP and Address Resolution Protocol (ARP) in an SMDS service environment configured as a logical IP subnetwork.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	Metropolitan Area Network (MAN)*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 1209	3/1/1991		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 1209	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.243) Transport Layer Security (TLS) Protocol

General Information

Website:	http://www.rfc-editor.org/rfcsearch.html
Description:	The Transport Layer Security (TLS) protocol provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0 (RFC 2246)	1/1/1999		
1.1 (RFC 4346)	4/1/2006		
1.2 (RFC 5246)	8/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.0 (RFC 2246)	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.244) TreeSize

General Information

Website:	http://www.jam-software.com/treesize/
Description:	TreeSize is a harddisk space manager. It shows you the size, allocated and wasted space, the number of files, 3D charts, the last access date, the file owner and permissions, the NTFS compression rate and much more information of several folders or drives you choose. It also lets you search drives, entire servers or the entire network for old, big, temporary and duplicate files.
Decision:	Approved
Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	JAM Software

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
4.3			
5.0	11/23/2007		
5.1	3/4/2008		
5.2	2/4/2009		
5.3	10/12/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
5.0	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo	Suppo

	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted	rted
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.245) Triple Data Encryption Algorithm (TDEA) Block Cipher

General Information

Website: http://csrc.nist.gov/publications/PubsSPs.html

Description: Triple Data Encryption Algorithm (TDEA) Block Cipher specifies the Triple Data Encryption Algorithm (TDEA), including its primary component cryptographic engine, the Data Encryption Algorithm (DEA). When implemented in an SP 800-38 series-compliant mode of operation and in a FIPS 140-2 compliant cryptographic module, TDEA may be used by Federal organizations to protect sensitive unclassified data. Protection of data during transmission or while in storage may be necessary to maintain the confidentiality and integrity of the information represented by the data. This recommendation precisely defines the mathematical steps required to cryptographically protect data using TDEA and to subsequently process such protected data.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: NIST

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	5/1/2004		
1.1	5/19/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the

responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.246) Uniform Resource Identifiers (URI)

General Information

Website: http://tools.ietf.org/html/rfc3986

Description: A Uniform Resource Identifier (URI) is a compact string of characters for identifying an abstract or physical resource. This standard defines the generic syntax of URI, including both absolute and relative forms, and guidelines for their use.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 3986	1/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on

the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 3986	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.247) Universal Description, Discovery, and Integration (UDDI)

General Information

Website: http://www.oasis-open.org/committees/uddi-spec/doc/tcspecs.htm

Description: The Universal Description, Discovery, and Integration (UDDI) specification describes the Web services, data structures and behaviors of all instances of a service registry.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: Benefits Arch

Decision Process: TRM v4.1

Decision Date: 10/28/2009

Current Status: Analysis Completed

Introduced By: Benefits ASA

Vendor Name: OASIS

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
UDDI Technical Specification	This document describes the Web services and behaviors of all instances of a UDDI registry.
UDDI XML Schema	UDDI uses the XML Schema Language to formally describe its data structures: • UDDI API Schema • UDDI Custody Schema • UDDI Subscription Schema • UDDI Subscription Listener Schema • UDDI Replication Schema • UDDI Value Set Validation Schema • UDDI Value Set Caching • UDDI Policy • UDDI Policy Instance parameters
UDDI WSDL Service Interface	The complete set of UDDI WSDL definitions is provided by: • UDDI API Binding • UDDI API Port Type • UDDI Custody Binding • UDDI Custody Port Type • UDDI Replication Binding • UDDI Replication Port Type • UDDI Subscription Binding • UDDI Subscription Port Type • UDDI Subscription Listener Binding • UDDI Subscription Listener Port Type • UDDI Value Set Validation Binding • UDDI Value Set Caching Binding • UDDI Value Set Caching Port Type

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interface	900: Service Discovery

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Web Services Description Language (WSDL) - Standard
- Extensible Markup Language (XML) - Standard
- XML Schema - Standard
- Simple Object Access Protocol (SOAP) - Standard
- WS-I Basic Profile - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2.0	7/19/2002		
3.0	10/19/2004		

VA Forecast Information (10/05/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009	CY2010	CY2011

Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
3.0	None	None	None	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. The Benefits Segment use of the UDDI specification is currently based on version 2.0.

General Analysis

Adoption Risks

- The implementation of UDDI based runtime registries in the industry is extremely limited. This raises a concern as to the value of this standard.

Architectural Benefits

- Provides a standardized interface specification for service discovery
- Interoperability - platform independent

Architectural Risks

- The standard only addresses storing metadata about content. This limits its capability to a Service Registry and does not address Service Repository capabilities.

Tier Used

- Middle Tier (Integration)

General Assessment

Expected Usage:	Service discovery
Assessment Type:	New
Assessment Date:	11/3/2009
Notes:	Architectural analysis needs to be conducted to determine whether there is a need in the VA for an integrated service registry/repository. If the analysis determines value in an integrated registry/repository then the ebXML Registry standard needs be assessed as UDDI would be insufficient. This analysis also needs to include other registry/repository requirements to determine if this standard is suitable.
Recommendation:	Approve

Recommendation Constraints:	
Recommendation Justification:	UDDI is a mature industry standard. It provides a standardized interface specification for a service registry.

4.248) Universal Healthcare Identifier (UHID)

General Information

Website:	http://www.astm.org/Standards/E1714.htm
Description:	ASTM E1714: Standard Guide for Properties of a Universal Healthcare Identifier (UHID) defines a set of requirements outlining the properties required to create a UHID.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ASTM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
E1714-95	10/15/1995		
E1714-00	10/10/2000		
E1714-07	8/15/2007		

VA Forecast Information (10/05/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. The Benefits Segment use of the UDDI specification is currently based on version 2.0.

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.249) UNIX

General Information

Website:	http://www.unix.org/
Description:	ISO/IEC 9945 & IEEE 1003.1: The Single UNIX Specification is the defacto and dejure standard definition for the UNIX system application programming interfaces.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	The Open Group

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code

Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2	3/12/1997		
3	1/30/2002		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
3	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.250) Unsolicited Email

General Information

Description: Unsolicited e-mails congest and restrict the availability of the network to work at acceptable performance levels. SPAM is defined as: to post irrelevant or inappropriate messages to one or more Usenet newsgroups, mailing lists,or other messaging system in a deliberate or accidental manner.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Anti-SPAM Software Deployment		All E-mail servers shall employ anti-SPAM software
Anti-SPAM Software Updates		SPAM detection signatures shall be downloaded and installed at least monthly.
Anti-SPAM		Anti-SPAM software shall be configured to run in a

Software Configuration		background mode.
Procedures		Procedures shall be implemented to: • Scal all emails upon access • Scall all emails before they are transmitted to another machine • Scan all emails incoming to the domain

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Outgoing E-mail Scanning	E-mails should be SPAM scanned before they are delivered to outgoing e-mail. A record of the time and date of the scan as well as the tool used should be included inthe body of the e-mail.
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) ACT

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.251) User Datagram Protocol (UDP)

General Information

Website: http://tools.ietf.org/html/rfc768

Description: The User Datagram Protocol (UDP) is one of the core members of the Internet Protocol Suite, the set of network protocols used for the Internet. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without requiring prior communications to set up special transmission channels or data paths.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 768	8/28/1980		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 768	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.252) vConverter

General Information

Website: http://www.vizioncore.com/products/vConverter/index.php

Description: vConverter provides numerous features for effective ongoing disaster recovery in existing physical environments; vConverter generates virtual backups for physical servers; vConverter's Continuous Protection Mode regularly updates these virtual backups with changes occurring on the physical server; vConverter ensures that a "virtual standby system" that is up to date and can be immediately utilized in the event of physical server problems or outages.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: CDCO Supported Architecture Components

Vendor Name: Quest Software

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Business Logic	891: Platform Dependent Technologies

Operating Systems Supported

- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.0	12/10/2007		
4.0	11/5/2008		
4.1	2/18/2009		
4.2	7/9/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
4.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.253) Veritas Storage Foundation

General Information

Website:	http://www.symantec.com/business/storage-foundation
Description:	Veritas Storage Foundation is an online storage management solution. It allows centralized management of diverse applications, servers and storage.
Decision:	Approved
Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	Symantec

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Business Logic	890: Platform Independent Technologies

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
4.1	4/15/2005		
5.0	6/23/2006		
5.1	12/7/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
5.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.254) Video Codec for Audiovisual Services

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=H

Description: ITU-T H.261: Video Codec for Audiovisual Services at p x 64 kbit/s describes the video coding and decoding methods for the moving picture component of audiovisual services at the rates of p x 64 kbit/s, where p is in the range 1 to 30.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: ITU

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	872: Media Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3	3/12/1993		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be

supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
3	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.255) Virtual Bridged Local Area Networks (VLAN)

General Information

Website: https://sbwsweb.ieee.org/ecustomercme_enu/start.swe?SWENeedContext=false&SWECmd=GotoPageTab&W=t&SWEC=3&SWEScrnCap=Standards&SWEBID=-1&SWETS=1270586674437&SWEScreen=Catalog_Standards_Screen_IEEE&SWEHo=sbwsweb.ieee.org&SWETS=1270586678508&SWEC=3

Description: IEEE 802.1Q: Virtual Bridged Local Area Networks (VLAN) specifies how the MAC Service is supported by Virtual Bridged Local Area Networks, the principles of operation of those networks, and the operation of VLAN-aware Bridges, including management, protocols, and algorithms.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IEEE

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	Campus Area Network (CAN)*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1998	1/1/1998		

2005	1/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2005	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.256) VLAN Trunking Protocol (VTP)

General Information

Website: http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094c52.shtml

Description: VLAN Trunking Protocol (VTP) is a Cisco proprietary Layer 2 messaging protocol that manages the addition, deletion, and renaming of Virtual Local Area Networks (VLAN) on a network-wide basis.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	Cisco

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	863: Service Transport

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1			
2			
3			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.257) VM Performance Toolkit

General Information

Website: http://www.vm.ibm.com/related/perfkit/

Description: The Performance Toolkit for VM provides enhanced capabilities for a z/VM systems programmer, system operator, or performance analyst to monitor and report performance data.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision CDCO

Source:	
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	866: Dependent Platform

Operating Systems Supported

- z/VM

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

VA forecast information is not available for this entry.

Forecast Note:	Refer to z/VM for release and VA Forecast information

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.258) VMware Site Recovery Manager

General Information

Website: http://www.vmware.com/products/site-recovery-manager/

Description: VMware Site Recovery Manager provides automated recovery process capabilities.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision CDCO 6.15.2009

Process:
Decision Date: 6/15/2009
Current Status: Analysis Completed
Introduced By: CDCO Supported Architecture Components
Vendor Name: VMware

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- VMware vSphere - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	6/16/2008		
4.0	10/5/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.259) VMware vCenter CapcityIQ

General Information

Website: http://www.vmware.com/products/vcenter-capacityiq/

Description: VMware vCenter CapcityIQ provides capacity management capabilities for virtualized datacenter or desktop environments.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	VMware

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- VMware vSphere - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	10/19/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.260) VMware vCenter Chargeback

General Information

Website: http://www.vmware.com/products/vcenter-chargeback/

Description: VMware vCenter Chargeback provides cost measurement, analysis and reporting capabilities of the virtual infrastructure.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision CDCO 6.15.2009

Process:
Decision Date: 6/15/2009
Current Status: Analysis Completed
Introduced By: CDCO Supported Architecture Components
Vendor Name: VMware

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- VMware vSphere - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	7/13/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.0	None	None	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.261) VMware vCenter Lab Manager

General Information

Website: http://www.vmware.com/products/labmanager/

Description: VMware vCenter Lab Manager provides on-demand access and automated management of the private cloud for development and test environments.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	VMware

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- VMware vSphere - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2.5	7/9/2007		
3.0	9/12/2008		
4.0	12/10/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
3.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.262) VMware vCenter Server Heartbeat

General Information

Website: http://www.vmware.com/products/vcenter-server-heartbeat/

Description: VMware vCenter Server Heartbeat detects standard VMware vCenter Server components upon installation, providing instant monitoring and protection.

Decision: Approved

Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	VMware

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- VMware vSphere - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.5	12/31/2007		
4.0	5/21/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
3.5	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.263) VMware vSphere

General Information

Website: http://www.vmware.com/products/vsphere/

Description: VMware vSphere, formerly known as VMware Infrastructure, provides management capability for large pools of virtualized

computing infrastructure, including software and hardware.

Decision: Approved

Decision Constraints: This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).

Decision Source: CDCO

Decision Process: CDCO 6.15.2009

Decision Date: 6/15/2009

Current Status: Analysis Completed

Introduced By: CDCO Supported Architecture Components

Vendor Name: VMware

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2.0	1/24/2008		
2.1	5/7/2008		
3.0	1/29/2009		
3.1	9/4/2009		
4.0	2/18/2010		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
3.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.264) VPN Services

General Information

Description: Virtual Private Network (VPN) is a service that allows authorized users to access a protected network from an untrusted network.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
RAS		The use of RAS is no longer the preferred method of accessing protected VA infrastructure or assets. VA approved VPN services are the preferred access method for authorized users of the VA network who must access protected assets from outside the One-VA Network.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
IETF RFC 2547	Border Gateway Protocol (BGP)/Multiprotocol Label Switching (MPLS) VPNs
IETF RFC 2917	A Core MPLS IP VPN Architecture

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.265) vRanger Pro

General Information

Website:	http://www.vizioncore.com/products/vRangerPro/
Description:	vRanger Pro is a virtual backup and recovery solution.
Decision:	Approved
Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	Quest Software

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Business Logic	891: Platform Dependent Technologies

Operating Systems Supported

- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- SQL Server related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
3.0	1/19/2007		
3.2	9/26/2007		
3.3	6/23/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on

the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
3.2	None	None	None	None	None	None	None	None	None	None	None	None
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.266) Warehouse Services

General Information

Description: Warehouse services are a subject-oriented, integrated, time-variant, non-volatile collection of structured and non-structured data used to support the strategicdecision-making process for the enterprise. It is the central point of data integration for business intelligence delivering a common view of enterprise data.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Database/Storage	Warehouse Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.267) Web Services Description Language (WSDL)

General Information

Website: http://www.w3.org/TR/

Description: The Web Services Description Language (WSDL) is an XML-based language that provides a specification for describing Web services. WSDL defines the logical and physical interface of a service: what the service does and how one can access it. The WSDL defines services as collections of network endpoints in an XML format. A client program connecting to a web service can read the WSDL to determine what functions are available at another endpoint. The client can then use SOAP (or some other protocol) to call one of the

functions listed in the WSDL.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: ARB

Decision Process: TRM v2

Decision Date: 9/17/2008

Current Status: Analysis Completed

Introduced By: TRM Team

Vendor Name: W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Core Langage	This specification defines the core language which can be used to describe Web services based on an abstract model of what the service offers. It also defines the conformance criteria for documents in this language.
Adjuncts	This specification specifies predefined extensions for use in WSDL 2.0: Message exchange patterns, Operation safety, Operation styles, and Binding extensions for SOAP and HTTP.
Primer	This primer is a starting point toward the use of WSDL.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interface	901: Service Description / Interface

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- WS-I Basic Profile - Standard
- Extensible Markup Language (XML) - Standard
- XML-Infoset - Standard
- XML Namespaces (XML-NS) - Standard
- XML Schema - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	9/1/2000		
1.1	3/15/2001		
1.2	7/9/2002		
2.0	6/26/2007		

VA Forecast Information (09/10/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**

1.2	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
2.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment use of the WSDL specification is currently based on version 1.1

General Analysis

Architectural Area

- Application
- Integration

Architectural Benefits

- Decoupling: A Service Consumer does not need to know anything about how the service is implemented. All the information required to use the service is contained in the contract (WSDL description of the Service). This separation of interface from implementation is at the heart of SOA.
- Interoperability: Service requests from any platform can read the WSDL, inspect the API and based on that inspection make calls to the described Service.
- Easy of development: All SOA-enabled IDEs can deal with WSDL, and generate a proxy class for the desired programming language (.NET, C#, VB, Java, etc.).
- Validation: While building request and response messages around XML schemas, WSDL can provide validation that the incoming message conforms to the schema.

Architectural Risks

- None significant.

EA Requirement

- ENTR 798 (Inactive) - VA/DoD Goal 4 - Integrated Information Sharing - Enable the efficient sharing of beneficiary data, medical records, and other information through secure and interoperable information management systems.
- ENTR 1074 - Implement a One VA information technology framework that supports the integration of information across business lines and that provides a source of consistent, reliable, accurate, and secure information to veterans and their families, employees, and stakeholders (Enabling Objective E-3).
- ENTR 821 (Inactive) - VHA Enabling Objective 18 - Develop innovative approaches to the design and evaluation of health care delivery systems.
- ENTR 794 (Inactive) - VHA Objective 3 - Optimize the use of health care information and technology for the benefit of the veteran.

Tier Used

- Integration Tier

Tool Usage

- Runtime - Embedded
- Development

General Assessment

Expected Usage:	WSDL is the specification for defining a web service description. In the SOA framework, WSDL can be an effective service contract between a provider and a consumer.
Assessment Type:	Standard
Assessment Date:	9/16/2008
Notes:	
Recommendation:	N/A
Recommendation Constraints:	
Recommendation Justification:	

4.268) WebLogic Server

General Information

Website:	http://www.oracle.com/appserver/weblogic/weblogic-suite.html
Description:	WebLogic Enterprise is now WebLogic Server, a foundational element of the WebLogic application platform. The WebLogic Service is a Java Enterprise Edition application server platform, designed to host distributed applications written using Java and the Java Enterprise Edition frameworks. The WebLogic Platform also includes Integration, Portal, Blended Frameworks and Workshop IDE.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	ARB

Decision Process:	TRM v2
Decision Date:	9/17/2008
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	Oracle

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	873: Application Servers

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required for some configurations)***
- Web Services Description Language (WSDL) - ***(required for some configurations)***
- Simple Object Access Protocol (SOAP) - ***(required for some configurations)***
- WS-Security - ***(required for some configurations)***
- Extensible Markup Language (XML) - ***(required for some configurations)***
- Universal Description, Discovery, and Integration (UDDI) - ***(required for some configurations)***
- WS-I Basic Profile - ***(required for some configurations)***
- WS-Reliable Messaging - ***(required for some configurations)***

- XSL Transformations (XSLT) - ***(required for some configurations)***
- XQuery - ***(required for some configurations)***
- Java EE - ***(required for some configurations)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
7.0	6/29/2002	4/15/2009	4/15/2011
8.1	7/15/2003	9/30/2009	9/30/2011
9.2	11/28/2006	11/30/2011	11/30/2013
10.2	2/15/2008	3/31/2013	3/31/2015
10.3	9/1/2008	3/31/2013	3/31/2015
11g (10.3.1)	7/1/2009		

VA Forecast Information (09/30/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
8.1	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
9.2	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**

10.3	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
11g (10.3.1)	None	None	None	None	None	**Planning**	**Evaluation**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment development and deployment of WebLogic Server is currently based on version 10.3.

General Analysis

Architectural Area

- Application
- Integration

Architectural Benefits

- The WebLogic application server provides a platform independent mechanism for developing, deploying and running HeV applications.
- The vendor appears to be committed to Java EE standards and provides commercial support.
- WebLogic Server is commercially available and Java EE compliant.

Architectural Risks

- The Oracle purchase of BEA creates unknowns about how WebLogic will fit-in with the Oracle fusion middleware.

EA Requirement

- Deploy an SOA compliant Java EE application server.

Standards Traceability

- JAX-WS 2.0
- JAXB 2.0
- Java EE 5
- EJB 3.0
- Java Persistence API (JPA)

Tier Used

- Middle Tier (Infrastructure)
- Client Tier
- Presentation Tier (Web)
- Middle Tier (Business)

- Middle Tier (Integration)

Tool Type

- Platform

Tool Usage

- Development
- Management/Collaboration
- Runtime

General Assessment

Expected Usage:	To provide a Java EE compliant application server on which to deploy and run Java EE based applications.
Assessment Type:	Refresh
Assessment Date:	9/5/2008
Notes:	WebLogic Server is one element of the WebLogic Platform that includes: Portal, Integration, Workshop IDE, JRockit, and other technologies. Only WebLogic server is in the scope of this assessment.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	Continue with WebLogic Server.

4.269) Wide Area Network (WAN)

General Information

Refer to document:	VA_Enterprise_IT_Infrastructure_Standard_WAN_1_0.pdf
Description:	This standards document lists the acceptable and recommended specifications for Wide Area Network. Sections include standard specifications for subject components, decisions supporting the standard specifications, guidelines or recommendations for implementing the standard specifications, and supplemental factors

to consider when evaluating subject components. Other supplementary documents will provide guidance on procuring components that meet the standard specifications, guidance on integrating them with existing components, and explanation of how the subject components fit into the VA Architecture.

This standard includes the following: Class A Router (Chassis; Packet Processor; Interface Cards; Operating System; WAN Encryption; Platform Supportability; Platform Maturity); Class B Router (Chassis; Packet Processor; Interface Cards; Operating System; WAN Encryption; Platform Supportability; Platform Maturity); Wide Area Network (Metro Data Center To Backbone; Metro Data Center to Region WAN; Medical Center to Region WAN; Medical Center Branch Office to Region WAN); WAN Encryption (Data Center; Medical Center); WAN Acceleration (Data Center; Medical Center).

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EIE CTO

Decision Process: TAR-TAS

Decision Date: 11/30/2009

Current Status: Analysis Completed

Introduced By: OPS/EIE

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	880: Wide Area Networks (WAN)

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
Vendor release information is not available for this entry.			

VA Forecast Information (09/30/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment development and deployment of WebLogic Server is currently based on version 10.3.											

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.270) Wi-Fi Protected Access (WPA)

General Information

Website:	http://www.wi-fi.org/knowledge_center/wpa2
Description:	Wi-Fi Protected Access (WPA) provides network administrators with a high level of assurance that only authorized users can access the network. Based on the ratified IEEE 802.11i standard, WPA provides government grade security by implementing the National Institute of Standards and Technology NIST FIPS 140-2 compliant AES encryption algorithm.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	Wi-Fi Alliance

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code

Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
WPA	4/1/2003		
WPA2	9/2/2004		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
WPA 2	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

Forecast Note:	

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.271) Wily Introscope

General Information

Website:	http://www.ca.com/us/application-management.aspx
Description:	Wily Introscope is an application management product that allows monitoring, proactive detection, triage and diagnosis of performance problems in complex, composite and Web application environments.
Decision:	Approved
Decision Constraints:	This technology's assessment and approval only applies to systems deployed at sites managed by the Corporate Data Center Operations (CDCO).
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	CA

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Enterprise Manager	The Enterprise Manager (EM) acts as the central repository for all Introscope performance data and metrics collected in an application environment. The EM processes performance data and makes it available to users for production monitoring and diagnosis.
WebView	Introscope WebView presents Web-based graphical UI to display Introscope performance data. Introscope's customizable dashboards and Explorer tree views for authorized users run in a browser interface, so that critical information can be viewed by those who need it anytime, anywhere. Note that the WebView component requires the Adobe SVG Viewer browser plug-in to display performance data.
Agent	Introscope agents collect performance metrics from the various components inside the running Web application, the application server and performance and availability data from the surrounding computing environment. The agents then report these metrics to the Enterprise Manager.
Workstation	The user controls Introscope and accesses performance metrics through the Introscope Workstation. Users can set alerts for individual metrics or logical metric groups, view performance metrics, and customize views to represent their unique environment. The Introscope Workstation has a Swing-based UI, for onsite or in-house use only

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- BMC Performance Manager
- Foglight

Companion Technologies/Standards:

- Apache Commons related as: (Companion)
- Apache Tomcat related as: (Companion)
- JasperReports related as: (Companion)
- Log4J related as: (Companion)
- JRE - Sun related as: (Companion)
- JAXB Reference Implementation related as: (Companion)

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
7.2			
8	6/16/2008		
8.1			

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.272) Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY)

General Information

Website: http://standards.ieee.org/getieee802/download/802.11-2007.pdf

Description: IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) defines the standard for wireless local area networks (WLANS).

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IEEE

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Hardware/Infrastructure	881: Local Area Networks (LAN)
Service Platform and Infrastructure	Hardware/Infrastructure	Campus Area Network (CAN)*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2003	1/1/2003		
2007	6/12/2007		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2003	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.273) Wireless Mobile Voice

General Information

Description: Consists of the software and protocols used for wireless and voice enabled presentation devices.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Policies

The following policies are associated with this entry:

Name	Source	Description
Security of External Electronic Connections	VA Directive 6212	This document describes the minimum security requirements for Department of Veterans Affairs (VA) external electronic connections.

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Web-centric	User Interfaces (UI) should be platform independent; therefore, the preferred approach to UIs on mobile devices is to use Web Client-Services via (micro) browsers.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	864: Wireless / Mobile

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

4.274) Wireless Transport Layer Security (WTLS)

General Information

Website:	http://www.openmobilealliance.org/tech/affiliates/wap/wapindex.html
Description:	WAP-261: Wireless Transport Layer Security Specification (WTLS) provides privacy, data integrity and authentication between two communicating applications. WTLS provides functionality similar to TLS 1.0 and incorporates new features such as datagram support, optimised handshake and dynamic key refreshing. The WTLS protocol is optimised for low-bandwidth bearer networks with relatively long latency.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	OMA

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
20010406	4/6/2001		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on

the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
20010406	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.275) WS-Reliable Messaging

General Information

Website: http://www.oasis-open.org/specs/#wsrx-rmv1.2

Description: The Web Services Reliable Messaging (WS-RM) specification describes a protocol that allows messages to be transferred reliably between nodes implementing this protocol in the presence of software component, system, or network failures. The protocol is described in this specification in a transport-independent manner allowing it to be implemented using different network technologies. To support interoperable Web services, a SOAP binding is defined within this specification.

The protocol defined in this specification depends upon other Web services specifications for the identification of service endpoint addresses and policies. How these are identified and retrieved are detailed within those specifications and are out of scope for this document.

By using the XML, SOAP, and WSDL extensibility model, SOAP-based and WSDL -based specifications are designed to be

composed with each other to define a rich Web services environment. As such, WS-ReliableMessaging by itself does not define all the features required for a complete messaging solution. WS-ReliableMessaging is a building block that is used in conjunction with other specifications and application-specific protocols to accommodate a wide variety of requirements and scenarios related to the operation of distributed Web services

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: Benefits Arch

Decision Process: TRM v4.1

Decision Date: 10/28/2009

Current Status: Analysis Completed

Introduced By: Benefits ASA

Vendor Name: OASIS

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- ebXML Messaging Service (ebMS)

Companion Technologies/Standards:

- Simple Object Access Protocol (SOAP) - Standard
- Web Services Description Language (WSDL) - Standard
- Extensible Markup Language (XML) - Standard
- XML Namespaces (XML-NS) - Standard
- XML Schema - Standard
- XML Path Language (XPath) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.1	1/7/2008		
1.2	9/10/2008		

VA Forecast Information (10/08/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.1	None	None	None	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Deprecated**	**Deprecated**	**Deprecated**	**Deprecated**
1.2	None	None	None	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment use of the WS-Reliable Messaging specification is currently based on version 1.1

General Analysis

Adoption Risks

- It currently has a limited industry implementation footprint.
- It is relatively new industry standard.

Architectural Benefits

- Transport independent protocol that support reliable delivery of messages.
- Supports reliable sequenced delivery of SOAP messages.

Tier Used

- Middle Tier (Infrastructure)
- Middle Tier (Integration)

General Assessment

Expected Usage:	Provide a protocol standard that allows SOAP messages to be reliably delivered between distributed applications in the presence of software component, system, or network failures.
Assessment Type:	New
Assessment Date:	11/3/2009
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	WS-RM provides a transport independent standard which enables Web Services to transmit sequences of messages across nodes reliably and in conformance with various rules called quality assurances.

4.276) WS-Security

General Information

Website:	http://www.oasis-open.org/specs/#wssv1.1
Description:	Web Services Security (WS-Security) describes enhancements to

SOAP messaging to provide message integrity and confidentiality. The specified mechanisms can be used to accommodate a wide variety of security models and encryption technologies.

This specification also provides a general-purpose mechanism for associating security tokens with message content. No specific type of security token is required, the specification is designed to be extensible (i.e. support multiple security token formats).

For example, a client might provide one format for proof of identity and provide another format for proof that they have a particular business certification.

Additionally, this specification describes how to encode binary security tokens, a framework for XML-based tokens, and how to include opaque encrypted keys. It also includes extensibility mechanisms that can be used to further describe the characteristics of the tokens that are included with a message.

Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	Benefits Arch
Decision Process:	TRM v4.1
Decision Date:	10/28/2009
Current Status:	Analysis Completed
Introduced By:	Benefits ASA
Vendor Name:	OASIS

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code

Component Framework	Security	885: Supporting Security Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Simple Object Access Protocol (SOAP) - Standard
- Extensible Markup Language (XML) - Standard
- XML Schema - Standard
- XML Namespaces (XML-NS) - Standard
- XML Path Language (XPath) - Standard
- Security Assertion Markup Language (SAML) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	3/15/2004		
1.1	2/21/2006		

VA Forecast Information (10/08/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Adoption Benefits

- WS-Security is a mature and widely adopted industry standard for securing Web Services.

Architectural Benefits

- WS-Security provides support for signing and encrypting SOAP messages.
- Messages can be protected from end to end, all the way from the original consumer, across any potential intermediaries on the message's path, to the provider and back again (unlike SSL/TLS where an intermediary would need to decrypt/process/encrypt the message).
- WS-Security supports the use of security tokens for SOAP messages.
- WS-Security defines communication protocol for secure web service message exchange (confidentiality, integrity, non-repudiation).

Tier Used

- Middle Tier (Infrastructure)

General Assessment

Expected Usage:	Standard communication protocol for securing Web Services.
Assessment Type:	New
Assessment Date:	11/3/2009
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation	WS-Security is a mature, widely adopted industry standard that provides end to end security for SOAP based messaging

Justification:

4.277) X.500 The Directory

General Information

Website: http://www.itu.int/itu-t/recommendations/index.aspx?ser=X

Description: ITU-T X.500: The Directory introduces the concepts of the Directory and the DIB (Directory Information Base) and overviews the services and capabilities which they provide.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Service Transport	862: Supporting Network Services

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
4	2/2/2001		
5	8/29/2005		
6	11/13/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
5	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.278) X.509 Certificate Request Message Format (CRMF)

General Information

Website: http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

Description: The Internet X.509 Certificate Request Message Format (CRMF) is used to convey a request for a certificate to a Certification Authority (CA), possibly via a Registration Authority (RA), for the purposes of X.509 certificate production. The request will typically include a public key and associated registration information.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2511	3/1/1999		
RFC 4211	9/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2511	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.279) X.509 PKI Representation of Key Exchange Algorithm (KEA) Keys

General Information

Website:	http://www.rfc-editor.org/cgi-bin/rfcsearch.pl
Description:	The Key Exchange Algorithm (KEA) is a classified algorithm for exchanging keys. This specification profiles the format and semantics of fields in X.509 V3 certificates containing KEA keys. The specification addresses the subject PublicKeyInfo field and the keyUsage extension.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2528	3/1/1999		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**

RFC 2528	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.280) X.509 Public Key Infrastructure (PKI) Certificate and CRL Profile

General Information

Website: http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

Description: The Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile describe the X.509 certificate and X.509 CRL for use in the Internet. The X.509 certificate format is described in detail, with additional information regarding the format and semantics of Internet name forms (e.g., IP addresses). Standard certificate extensions are described and one new Internet-specific extension is defined. A required set of certificate extensions is specified. The X.509 CRL format is described and a required extension set is defined as well. An algorithm for X.509 certificate path validation is described. Supplemental information is provided describing the format of public keys and digital signatures in X.509 certificates for common Internet public key encryption algorithms (i.e., RSA, DSA, and Diffie-Hellman).

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2459	1/1/1999		
RFC 3280	4/1/2002		
RFC 5280	5/1/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 3280	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.281) X.509 Public Key Infrastructure (PKI) Certificate Management Protocols

General Information

Website: http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

Description: The Internet X.509 Public Key Infrastructure (PKI) Certificate Management Protocols define the protocol messages for all relevant aspects of certificate creation and management.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008
Current Status: Analysis Completed
Introduced By: TRMSP
Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date

RFC 2510	3/1/1999		
RFC 4210	9/1/2005		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
RFC 2510	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.282) X.509 Public Key Infrastructure LDAP Schema

General Information

Website: http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

Description: The Internet X.509 Public Key Infrastructure LDAPv2 Schema is a minimal schema to support PKIX in an LDAPv2 environment. Only PKIX-specific components are specified. LDAP servers, acting as PKIX repositories should support the auxiliary object classes defined in this specification and integrate this schema specification with the generic and other application-specific schemas as appropriate, depending on the services to be supplied by that server.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2587	6/1/1999		
RFC 4523	6/1/2006		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2587	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.283) X.509 Public Key Infrastructure Online Certificate Status Protocol (OCSP)

General Information

Website: http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

Description: The Internet X.509 Public Key Infrastructure Online Certificate Status Protocol (OCSP) specifies a protocol useful in determining the current status of a digital certificate without requiring Certificate Revocation Lists (CRLs).

Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2560	6/1/1999		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2560	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.284) X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP

General Information

Website: http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

Description: Internet X.509 Public Key Infrastructure (PKI) Operational Protocols: FTP and HTTP specifies the conventions for using the File Transfer

Protocol (FTP) and the Hypertext Transfer Protocol (HTTP) to obtain certificates and Certificate Revocation Lists (CRLs) from PKI repositories.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
RFC 2585	5/1/1999		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
RFC 2585	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.285) X.509 Public Key Infrastructure Operational Protocols: LDAP

General Information

Website: http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

Description: The Internet X.509 Public Key Infrastructure Operational Protocols: LDAP - addresses requirements to provide access to Public Key Infrastructure (PKI) repositories for the purposes of retrieving PKI information and managing that same information. The mechanism is based on the Lightweight Directory Access Protocol (LDAP) defining a profile of that protocol for use within the IPKI and updates encodings for certificates and revocation lists.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRMSP

Vendor Name: IETF

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0 (RFC 2559)	4/1/1999		
2.0 (RFC 3494)	3/1/2003		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.0 (RFC 2559)	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.286) X.509 Public-Key and Attribute Certificate Frameworks

General Information

Website:	http://www.iso.org/iso/catalogue_detail.htm?csnumber=34551
Description:	ISO/IEC 9594-8, ITU-T X.509, & IETF RFC 3647: Public-Key and Attribute Certificate Frameworks defines a framework for public-key certificates and attribute certificates. These frameworks may be used by other standards bodies to profile their application to Public Key Infrastructures (PKI) and Privilege Management Infrastructures (PMI). Also, this standard defines a framework for the provision of authentication services by Directory to its users. It describes two levels of authentication: simple authentication, using a password as a verification of claimed identity; and strong authentication, involving credentials formed using cryptographic techniques. While simple authentication offers some limited protection against unauthorized access, only strong authentication should be used as the basis for providing secure services.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	ISO

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	Confidentiality Services*
Service Access and Delivery	Service Transport	IPv6 Stack Design*

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
4	3/31/2001		
5	1/1/2005		
5.1	1/13/2007		
5.2	11/13/2008		
6	11/13/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be

supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
5.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.287) XML Namespaces (XML-NS)

General Information

Website: http://www.w3.org/TR/xml-names11/

Description: XML Namespaces (XML-NS) provide a simple method for qualifying element and attribute names used in eXtensible Markup Language (XML) documents by associating them with namespaces identified by Internationalized Resource Identifier (IRI) references.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRM Team

Vendor Name: W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Extensible Markup Language (XML) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.1	8/16/2006		

VA Forecast Information (11/02/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be

supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.1	None	None	None	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Adoption Benefits

- Mature, widely adopted industry standard.

Architectural Benefits

- Reduction of XML markup vocabulary "collisions".
- Standardization/re-use of XML markup vocabularies.

General Assessment

Expected Usage:	Specification for XML element and attribute definitions.
Assessment Type:	Standard
Assessment Date:	11/2/2009
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	XML-NS provides a standard for XML markup vocabularies. Use of this standard will reduce the chances of namespace collisions.

4.288) XML Path Language (XPath)

General Information

Website: http://www.w3.org/TR/

Description: XML Path Language (Xpath) is an expression language that allows the processing of values conforming to the data model defined in Xquery/Xpath Data Model (XDM). The data model provides a tree representation of XML documents as well as atomic values such as integers, strings, and booleans, and sequences that may contain both references to nodes in an XML document and atomic values. The result of an Xpath expression may be a selection of nodes from the input documents, or an atomic value, or more generally, any sequence allowed by the data model. The name of the language derives from its most distinctive feature, the path expression, which provides a means of hierarchic addressing of the nodes in an XML tree.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRM Team

Vendor Name: W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
XQuery/XPath Data Model (XDM)	This document defines the W3C XQuery and XPath Data Model (XDM), which is the data model of XPath, XSLT, and XQuery, and any other specifications that reference it.
XQuery/XPath Functions & Operations	This document defines constructor functions, operators and functions on the datatypes defined in XML Schema Part 2: Datatypes and the datatypes defined in XQuery 1.0 and XPath 2.0 Data Model. It also

	discusses functions and operators on nodes and node sequences as defined in the XQuery 1.0 and XPath 2.0 Data Model.
XQuery/XPath Formal Semantics	This document defines formally the semantics of XQuery 1.0 and XPath 2.0.
XQuery/XPath Full Text	This document defines constructor functions, operators and functions on the datatypes defined in XML Schema Part 2: Datatypes and the datatypes defined in XQuery 1.0 and XPath 2.0 Data Model. It also discusses functions and operators on nodes and node sequences as defined in the XQuery 1.0 and XPath 2.0 Data Model.
XML Path Language	XPath is an expression language that allows the processing of values conforming to the data model defined in [XQuery/XPath Data Model (XDM)]. The data model provides a tree representation of XML documents as well as atomic values such as integers, strings, and booleans, and sequences that may contain both references to nodes in an XML document and atomic values. The result of an XPath expression may be a selection of nodes from the input documents, or an atomic value, or more generally, any sequence allowed by the data model.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Extensible Markup Language (XML) - Standard
- XML Namespaces (XML-NS) - Standard
- XML Schema - Standard
- XQuery - Standard
- XSL Transformations (XSLT) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	11/16/1999		
2.0	1/23/2007		

VA Forecast Information (11/02/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
2.0	None	None	None	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Adoption Benefits

- XPath is a mature and widely adopted industry standard for querying XML documents.
- The XPath language is simple and concise.

Architectural Benefits

- Provides a single syntax for querying XML documents.

Architectural Risks

- None identified at this time.

General Assessment

Expected XML Query language for querying XML documents.

Usage:	
Assessment Type:	New
Assessment Date:	11/2/2009
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	XPath is a mature, widely adopted industry standard for querying XML documents. XPath is concise, simple, and powerful.

4.289) XML Pointer Framework

General Information

Website:	http://www.w3.org/TR/xptr-framework/
Description:	The XML Pointer Language (XPointer) Framework is an extensible system for XML addressing that underlies additional XPointer scheme specifications.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP
Vendor Name:	W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	897: Data Format / Classification

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Extensible Markup Language (XML) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	3/25/2003		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.290) XML Schema

General Information

Website: http://www.w3.org/XML/Schema

Description: XML Schemas, also referred to as XML Schema Documents (XSDs), express shared vocabularies and allow machines to carry out rules made by people. They provide a means for defining the structure, content and semantics of XML documents in more detail.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: EA

Decision Process: TRMSP 4.3.2

Decision Date: 3/14/2008

Current Status: Analysis Completed

Introduced By: TRM Team

Vendor Name: W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

The following guidelines and best practices are associated with this entry:

Name	Description
Namespaces	Recommended XML Namespace for Government Organizations

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
Primer	Primer is a non-normative document intended to provide an easily readable description of the XML Schema facilities, and is oriented towards quickly understanding how to create schemas using the XML Schema language.
Structure	This document specifies the XML Schema definition language, which offers facilities for describing the structure and constraining the contents of XML 1.0 documents, including those which exploit the XML Namespace facility. The schema language, which is itself represented in XML 1.0 and uses namespaces, substantially reconstructs and considerably extends the capabilities found in XML 1.0 document type definitions (DTDs). This specification depends on XML Schema Part 2: Datatypes.
DataTypes	This document defines facilities for defining datatypes to be used in XML Schemas as well as other XML specifications. The datatype language, which is itself represented in XML 1.0, provides a superset of the capabilities found in XML 1.0 document type definitions (DTDs) for specifying datatypes on elements and attributes.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	898: Data Types / Validation

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Extensible Markup Language (XML) - Standard
- XML Namespaces (XML-NS) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	5/2/2001		
1.1	10/28/2004		

VA Forecast Information (11/02/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.1	None	None	None	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Adoption Benefits

- Mature, widely adopted industry standard

Adoption Risks

- Schemas can become verbose

Architectural Benefits

- XML content validation
- Strongly typed data structure definitions

General Assessment

Expected Usage:	Definition of structure, content, and semantics of XML based content.
Assessment Type:	Standard
Assessment Date:	11/2/2009
Notes:	
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	XML Schema is a mature, widely adopted industry standard that provides a specification for creating strongly type data structure definitions whose contents can be easily validated.

4.291) XML Signature Syntax and Processing (XML-Sig)

General Information

Website:	http://www.w3.org/TR/
Description:	XML Signature Syntax and Processing (XML-Sig) specifies XML digital signature processing rules and syntax. XML Signatures provide integrity, message authentication, and/or signer authentication services for data of any type, whether located within the XML that includes the signature or elsewhere.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	EA
Decision Process:	TRMSP 4.3.2
Decision Date:	3/14/2008
Current Status:	Analysis Completed
Introduced By:	TRMSP

Vendor Name: W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Security	884: Certificates / Digital Signature

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- Security Assertion Markup Language (SAML) - Standard
- Extensible Markup Language (XML) - Standard
- XML Namespaces (XML-NS) - Standard
- XML Path Language (XPath) - Standard
- XSL Transformations (XSLT) - Standard
- Multipurpose Internet Mail Extensions (MIME) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
IETF RFC 3275	3/1/2002		
1.0	2/12/2002		
2.0	6/10/2008		

VA Forecast Information (03/14/2008)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2010				CY2011				CY2012			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
IETF RFC 3275	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.292) XMLSpy

General Information

Website: http://www.altova.com/products/xmlspy/xml_editor.html

Description: XMLSpy is a markup language editor and integrated development environment for creating, modifying, transforming and debugging XML-related technologies. XMLSpy has a graphical schema designer, code generator, file converters, debuggers, profilers,

relational database integration, and Visual Studio and Eclipse plug-ins. XMLSpy supports several standards and specifications such as XLST, Xpath, XQuery, WSDL, SOAP, XBRL, and OOXML.

Decision: Approved

Decision Constraints: No constraints have been specified at this time.

Decision Source: ARB

Decision Process: TRM v3.1

Decision Date: 5/13/2009

Current Status: Analysis Complete

Introduced By: TRM Team

Vendor Name: Altova

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	867: Integrated Development Environments (IDE)

Operating Systems Supported

- Red Hat Linux
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Eclipse - ***(required for some configurations)***

- XML Path Language (XPath) - ***(required libraries)***
- XSL Transformations (XSLT) - ***(required libraries)***
- XQuery - ***(required libraries)***
- XML Schema - ***(required libraries)***
- Extensible Markup Language (XML) - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
2004	9/2/2003		
2004.3	10/28/2003		
2004.4	5/17/2004		
2005	10/3/2004		
2006	10/3/2005		
2006.3	6/1/2006		
2007	10/24/2006		
2007.3	5/30/2007		
2008	9/12/2007		
2008.2	4/29/2008		
2009	2/3/2009		

VA Forecast Information (10/27/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2004	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
2005	Supported	Supported	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
2009	None	None	Planning	Evaluation	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Forecast Note:	The information displayed in the above forecast table does not apply to the Benefits Segment. Benefits Segment use of XML Spy is currently based on version 2005.

General Analysis

Architectural Area

- Application
- Integration
- Data

Architectural Benefits

- Common developer toolsets which support standardized skill sets, the implementation of best practices, as well as improvements in developer efficiency and effectiveness; all contribute to the architectural goals of reduced development risks and repeatable, consistent development practices for HeV.

EA Requirement

- ENTR909 - All applications and services shall reference the VHIM Template Registry (VTS) as the authoritative source/store for all VHIM implementation artifacts such as XML Schema Documents (XSD) and other metadata.
- ENTR1274 - Systems implementing VHA security audit shall be capable of converting standard audit to all of the following formats- XML, XLS, TXT, Comma Separated Value (CSV), DataBase File (DBF).
- ENTR1074 - VA OBJECTIVE E.3 Implement a One-VA information technology framework that enables the consolidation of IT solutions and the creation of cross-cutting common services to support the integration of information across business lines and provides secure, consistent, reliable, and accurate information to all interested parties.

Tool Type

- Tool

Tool Usage

- Development

General Assessment

Expected Usage:	A commercial XML integrated development environment for development XML documents and specifications.
Assessment Type:	New
Assessment Date:	3/9/2009
Notes:	XMLSpy is a component of a larger bundle of development tools offered by Altova. Altova offers two suites of products, 2 different Mission Kits, which is targeted towards software architects and includes support for XML and web services development, data mapping and integration, publishing, UML modeling and database query and design. The 2nd Mission Kit is targeted at developers and doesn't include UML modeling or database query and design support.
Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	XMLSpy is a recognized industry leader for XML related development and support technologies.

4.293) XQuery

General Information

Website:	http://beta.w3.org/standards/techs/xquery
Description:	XQuery is a query and functional programming language that is designed to query collections of XML data. XQuery is an extension of XPath version 2.0. Any expression that is syntactically valid and executes successfully in both XPath 2.0 and XQuery will return the same result in both languages. Since these languages are so closely related, their grammars and language descriptions are generated from a common source to ensure consistency, and the editors of these specifications work closely together.

Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	Benefits Arch
Decision Process:	TRM v4.1
Decision Date:	10/28/2009
Current Status:	Analysis Completed
Introduced By:	Benefits ASA
Vendor Name:	W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

Note: The components of an approved entry are only allowed to be used in the context of the approved entry. The following components are included in the Approved decision:

Name	Description
XQuery/XPath Data Model (XDM)	This document defines the W3C XQuery and XPath Data Model (XDM), which is the data model of XPath, XSLT, and XQuery, and any other specifications that reference it.
XQuery/XPath Functions & Operations	This document defines constructor functions, operators and functions on the datatypes defined in XML Schema Part 2: Datatypes and the datatypes defined in XQuery 1.0 and XPath 2.0 Data Model. It also discusses functions and operators on nodes and node sequences as defined in the XQuery 1.0 and XPath 2.0 Data Model.
XQuery/XPath Formal Semantics	This document defines formally the semantics of XQuery and XPath.
XQuery/XPath Full Text	This document defines constructor functions, operators and functions on the datatypes defined in XML Schema Part 2: Datatypes and the datatypes defined in XQuery 1.0 and XPath 2.0 Data Model. It also discusses functions and operators on nodes and node sequences as defined in the XQuery 1.0 and XPath 2.0 Data Model.
XQuery 1.0: An XML Query Language	XML is a versatile markup language, capable of labeling the information content of diverse data sources including structured and semi-structured documents, relational databases, and object repositories. A query language that uses the structure of XML intelligently can express queries

	across all these kinds of data, whether physically stored in XML or viewed as XML via middleware. This specification describes a query language called XQuery, which is designed to be broadly applicable across many types of XML data sources.

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Interchange	892: Data Exchange

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Structured Query Language (SQL)
- XSL Transformations (XSLT)

Companion Technologies/Standards:

- Extensible Markup Language (XML) - Standard
- XML Namespaces (XML-NS) - Standard
- XML Schema - Standard
- XML Path Language (XPath) - Standard
- XLink - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	1/23/2007		

VA Forecast Information (10/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on

the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.0	None	None	None	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Adoption Benefits

- XQuery is a widely adopted industry standard
- XQuery is easier to learn than XSLT

Adoption Risks

- XQuery is limited to static analysis as it lacks dynamic binding

Architectural Benefits

- Data Integration - provides select, filter, transform, join, and aggregate data capabilities across multiple data sources
- Expressiveness - XQuery can query many different data structures and its recursive nature makes it ideal for querying tree and graph structures
- Brevity - XQuery statements are shorter than similar SQL or XSLT programs
- Flexibility - XQuery can query both hierarchical and tabular data
- Consistency - XQuery has a consistent syntax and can be used with other XML standards such as XML Schema datatypes

General Assessment

Expected Usage:	To extract and manipulate data from XML documents or any data source that can be viewed as XML.
Assessment Type:	Standard
Assessment Date:	11/2/2009
Notes:	

Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	XQuery is a widely adopted industry standard for finding, extracting and manipulating data from XML documents. It provides a powerful database query capability similar to that of SQL.

4.294) XSL Transformations (XSLT)

General Information

Website:	http://www.w3.org/TR/xslt20
Description:	The XSL Transformations (XSLT) specification defines the syntax and semantics of XSLT 2.0, a language for transforming XML documents into other XML documents. XSLT 2.0 is designed to be used in conjunction with XPath 2.0. XSLT shares the same data model as XPath 2.0 and it uses the library of functions and operators defined in Xpath. XSLT 2.0 also includes optional facilities to serialize the results of a transformation, by means of an interface to the serialization component.
Decision:	Approved
Decision Constraints:	No constraints have been specified at this time.
Decision Source:	Benefits Arch
Decision Process:	TRM v4.1
Decision Date:	10/28/2009
Current Status:	Analysis Completed
Introduced By:	Benefits ASA
Vendor Name:	W3C

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Interoperability	899: Data Transformation

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- XQuery

Companion Technologies/Standards:

- Extensible Markup Language (XML) - Standard
- XML-Infoset - Standard
- XML Namespaces (XML-NS) - Standard
- XML Schema - Standard
- XML Path Language (XPath) - Standard

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.0	11/16/1999		
2.0	1/23/2007		

VA Forecast Information (10/05/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on

the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2.0	None	None	None	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Adoption Benefits

- XSLT is a mature and widely adopted industry standard for transforming XML documents.

Adoption Risks

- Declarative languages such as XSLT may incur a performance penalty and require greater resources.

Architectural Benefits

- XSLT applications for transforming XML data structures can be made much more resilient to changes in the details of the XML documents than a procedural application coded using the low-level DOM and SAX interfaces. This leads to data independence.
- Supports multiple output processing from a single XSLT transformation, enabling the production of multiple instances of XML, HTML, xHTML, or text outputs. This increases interoperability.
- Supports multiple input processing, including non-XML formats such as HTML, xHTML, and delimited files. This increases interoperability.

General Assessment

Expected Usage:	Support XML document transformation requirements.
Assessment Type:	New
Assessment Date:	11/18/2009
Notes:	

Recommendation:	Approve
Recommendation Constraints:	
Recommendation Justification:	XSLT is a mature, widely adopted industry standard. It provides a specification for transforming XML documents.

4.295) z/OS

General Information

Website:	http://www-03.ibm.com/systems/z/os/zos/
Description:	z/OS is a 64-bit graphical user interface based operating system for mainframe computers. It is the successor to OS/390, which in turn followed MVS and combined a number of formerly separate, related products.
Decision:	Approved
Decision Constraints:	Products that have been deployed to a production environment may continue to use this technology. All other products must utilize a One-VA TRM approved Linux operating system.
Decision Source:	CDCO
Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	866: Dependent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
1.5	3/26/2004		3/31/2007
1.6	9/24/2004		9/30/2007
1.7	9/30/2005		9/30/2008
1.8	9/29/2006		9/30/2009
1.9	9/28/2007		9/30/2010
1.10	9/26/2008		
1.11	9/25/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or

production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1.5	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.6	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.7	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.8	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.9	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Deprecated	Deprecated	Deprecated	Deprecated	Deprecated
1.10	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

4.296) z/VM

General Information

Website: http://www.vm.ibm.com/

Description: z/VM is a 64-bit virtual machine operating system. It can be used to support large numbers (thousands) of Linux virtual machines.

Decision: Approved

Decision Constraints: Products that have been deployed to a production environment may continue to use this technology. All other products must utilize a One-VA TRM approved Linux operating system.

Decision Source: CDCO

Decision Process:	CDCO 6.15.2009
Decision Date:	6/15/2009
Current Status:	Analysis Completed
Introduced By:	CDCO Supported Architecture Components
Vendor Name:	IBM

Policies

No policies have been identified for this entry

Guidelines and Best Practices

No guidelines have been identified for this entry

Components

No components have been identified for this entry

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	866: Dependent Platform

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

Companion Technologies/Standards:

- No companion products have been identified at this time.

Vendor Release Information

The Vendor Release table provides the known releases for the TRM technology/standard, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
5.3	6/29/2007		
5.4	9/12/2008		
6.1	10/23/2009		

VA Forecast Information (06/15/2009)

The VA Forecast offers the current and future VA IT position regarding different releases of the TRM entry. The forecast is based on the best information-judgment on the current forecast date (see above). The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and-or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Forecast Information is considered prohibited from use.

	CY2009				CY2010				CY2011			
Release	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
5.3	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Forecast Note:												

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

5) Prohibited Technologies/Standards List

Name	Vendor	Deciding Source	Decision Process	Decision Date
Abbot Java GUI Test Framework	N/A	ARB	TRM v4	9/16/2009
AOPAlliance	N/A	ARB	TRM v3	1/7/2009
AspectJ	Eclipse	ARB	TRM v3	1/7/2009
Beehive	ASF	HSD&D	ETL	12/1/2006
Cache Objects	InterSystems	HSD&D	ETL	12/1/2006

CVS	N/A	HSD&D	ETL	12/1/2006
Datafile	N/A	ARB	TRM v4.1	10/28/2009
Dreamweaver	Adobe	ARB	TRM v3	1/7/2009
Drools	JBoss	ARB	TRM v3.2	8/19/2009
GroboUtils	N/A	ARB	TRM v4.1	10/28/2009
i-net JDBC Drivers	i-net software	ARB	TRM v4	9/16/2009
Jakarta Object Relational Bridge	ASF	HSD&D	ETL	12/1/2006
JavaServer Faces Reference Implementation	Sun Microsystems	HSD&D	ETL	12/1/2006
JBoss	RedHat	HSD&D	ETL	12/1/2006
jBPM	RedHat	ARB	TRM v4.1	10/28/2009
JDK - JRockit	Oracle	ARB	TRM v3	1/7/2009
JRE - JRockit	Oracle	ARB	TRM v3	1/7/2009
M2Eclipse	N/A	ARB	TRM v4.1	10/28/2009
Maven	ASF	ARB	TRM v3	1/7/2009
MediaWiki	Wikimedia Foundation, Inc.	ARB	TRM v3.2	8/19/2009
MetaHelper	N/A	ARB	TRM v4	9/16/2009
MySQL	Sun Microsystems	HSD&D	ETL	12/1/2006
Oracle Data Service Integrator	Oracle	HSD&D	ETL	12/1/2006
PDF Renderer	N/A	ARB	TRM v4.1	10/28/2009
Perforce	Perforce Software	HSD&D	ETL	12/1/2006
Rational XDE Developer	IBM	HSD&D	ETL	12/1/2006
Rational XDE Tester	IBM	HSD&D	ETL	12/1/2006
TestNG	TestNG	ARB	TRM v4	9/16/2009
TPTP	Eclipse	ARB	TRM v4.1	10/28/2009
Tuxedo	Oracle	HSD&D	ETL	12/1/2006
TWiki	Twiki.net	ARB	TRM v3.2	8/19/2009

6) Prohibited Technologies/Standards Entries

6.1) Abbot Java GUI Test Framework

General Information

Website: http://abbot.sourceforge.net/doc/overview.shtml

Description: Abbot Framework is a Graphical User Interface testing framework designed to facilitate-automate the testing of Java user interfaces, such as implemented using Java Swing. The framework is comprised of Abbot, a programmatic interface for testing and Costello, built on Abbot. The framework includes a UI for launching, exploring and controlling an application.

Decision: Prohibited

Decision Constraints:

Decision Source: ARB

Decision Process: TRM v4

Decision Date: 9/16/2009

Current Status: Introduced

Introduced By: ARB

Vendor Name: N/A

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	869: Test Management

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- Rational Functional Tester

General Analysis

Adoption Benefits

- Adoption of this technology will not increase the current benefits provided by Rational Functional Tester.

Adoption Risks

- Support for Abbott is currently only available through email and is based on community support.

Architectural Benefits

- Abbott provides an open source framework specifically targeted at testing Java user interfaces, which is not provided with JUnit. This fills the gap that exists when attempting to automate unit testing of Java user interfaces and supports Test Driven Development.

Architectural Risks

- Abbott is a point product (specific to Java user interface testing) it does not support other forms of user interface testing such as the web and does not necessarily align with the goals of the VA.
- Rational Functional Tester already covers the functionality being requested and adoption would result in multiple conflicting technologies in this area.

Tool Type

- Framework

Tool Usage

- Automated testing of Java user interfaces.

General Assessment

Expected Usage:	Automate testing of Java user interfaces implemented with Swing, JFC, etc.
Assessment	New

Type:	
Assessment Date:	8/5/2009
Notes:	
Recommendation:	Deny
Recommendation Constraints:	
Recommendation Justification:	Rational Functional Tester already provides the functionality needed to automate testing of Java user interfaces and does not warrant approval this technology at this time.

6.2) AOPAlliance

General Information

Website:	http://aopalliance.sourceforge.net/
Description:	AOP Alliance is a set of java based APIs for aspect oriented programming. **Note: The AOP Alliance APIs have been implemented in the Spring AOP framework. They are not permitted to be utilized independently of the Spring AOP framework in order to minimize the proliferation of disparate AOP technologies. The Spring Framework (Spring AOP) is the approved technology to support aspect oriented programming.**
Decision:	Prohibited
Decision Constraints:	
Decision Source:	ARB
Decision Process:	TRM v3
Decision Date:	1/7/2009
Current Status:	Introduced
Introduced By:	Extended Tool List (ETL)
Vendor Name:	N/A

FEA Categories

Service Area	Service Category	Service Standard Code

N/A	N/A	N/A

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Spring Framework

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

6.3) AspectJ

General Information

Website:	http://www.eclipse.org/aspectj/
Description:	AspectJ is an aspect-oriented extension to the Java programming language that enables modularization of 'crosscutting concerns' such as logging, error handling, standards enforcement, and feature variations **Note: AspectJ has been moved to the "Prohibited" status so that the use of static AOP is discouraged and the proliferation of disparate AOP technologies is minimized. The Spring Framework (Spring AOP) is the approved technology to support aspect oriented programming.**
Decision:	Prohibited
Decision Constraints:	
Decision Source:	ARB
Decision	TRM v3

Process:
Decision Date: 1/7/2009
Current Status: Introduced
Introduced By: Extended Tool List (ETL)
Vendor Name: Eclipse

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	895: Middleware

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Spring Framework

General Analysis

Analysis details are not available for this entry.

General Assessment

An assessment is not available for this technology.

6.4) Beehive

General Information

Website: http://beehive.apache.org/

Description: Beehive, formerly known as BEA Beehive, is an open-source set of ease-of-use frameworks for enterprise Java applications. Beehive is comprised of the following;
NetUI: An annotation-driven web application programming framework that is built atop Struts. NetUI centralizes navigation logic, state, metadata, and exception handling in a single

encapsulated and reusable Page Flow Controller class. In addition, NetUI provides a set of JSP tags for rendering HTML / XHTML and higher-level UI constructs such as data grids and trees and has first-class integration with JavaServer Faces and Struts.
Controls: A lightweight, metadata-driven component framework for building that reduces the complexity of being a client of enterprise resources. Controls provide a unified client abstraction that can be implemented to access a diverse set of enterprise resources using a single configuration model.
Web Service Metadata (WSM): An implementation of JSR 181 which standardizes a simplified, annotation-driven model for building Java web services.
In addition, Beehive includes a set of system controls that are abstractions for low-level J2EE resource APIs such as EJB, JMS, JDBC, and web services.

Decision: Prohibited

Decision Constraints:

Decision Source: HSD&D

Decision Process: ETL

Decision Date: 12/1/2006

Current Status: Introduced

Introduced By: Extended Tool List (ETL)

Vendor Name: ASF

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	895: Middleware

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

General Analysis

ETL Prohibited Technology/Standard, TRM Analysis still pending.

General Assessment

ETL Prohibited Technology/Standard, TRM Assessment still pending.

6.5) Cache Objects

General Information

Website: http://www.intersystems.com/cache/technology/techguide/cache_tech-guide_02.html#05

Description: Caché Objects is the object representation of data accessed from a Caché database. Caché data can be accessed as objects, relational tables, and multidimensional arrays.
Note: Caché based data should be accessed using SQL in order to reduce the effort needed to transition from Caché, a post-relational database, to a relational data base management system (RDBMS).

Decision: Prohibited

Decision Constraints:

Decision Source: HSD&D

Decision Process: ETL

Decision Date: 12/1/2006

Current Status: Introduced

Introduced By: Extended Tool List (ETL)

Vendor Name: InterSystems

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Database/Storage	875: Database

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

General Analysis

ETL Prohibited Technology/Standard, TRM Analysis still pending.

General Assessment

ETL Prohibited Technology/Standard, TRM Assessment still pending.

6.6) CVS

General Information

Website:	http://www.nongnu.org/cvs/
Description:	Concurrent Versions System (CVS) is a version control system that can record the history of source files and documents. **Note: Rational ClearCase with Multisite and Rational Team Concert are the approved technologies for version control.**
Decision:	Prohibited
Decision Constraints:	
Decision Source:	HSD&D
Decision Process:	ETL
Decision Date:	12/1/2006
Current Status:	Introduced
Introduced By:	Extended Tool List (ETL)

Vendor Name: N/A

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	868: Software Configuration Management

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Rational ClearCase with MultiSite
- Rational Team Concert

General Analysis

ETL Prohibited Technology/Standard, TRM Analysis still pending.

General Assessment

ETL Prohibited Technology/Standard, TRM Assessment still pending.

6.7) Datafile

General Information

Website: http://datafile.sourceforge.net/

Description: Datafile is a utility implemented in java that provides a set of interfaces for reading and writing data to and from files in several formats.

Decision: Prohibited

Decision Constraints:

Decision ARB

Source:	
Decision Process:	TRM v4.1
Decision Date:	10/28/2009
Current Status:	Analysis Completed
Introduced By:	ARB
Vendor Name:	N/A

FEA Categories

Service Area	Service Category	Service Standard Code
N/A	N/A	N/A

Operating Systems Supported

- Red Hat Linux
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

General Analysis

Adoption Benefits

- Standard functions for reading/writing files in various widely accepted formats.

Adoption Risks

- Datafile was written by a single developer, no support is available, and datafile has not been updated in over four years.

Architectural Benefits

- None significant.

Architectural Risks

- None significant.

General Assessment

Expected Usage:	Datafile is a java utility that provides the capability to read and write data in various formats.
Assessment Type:	New
Assessment Date:	10/9/2009
Notes:	
Recommendation:	Deny
Recommendation Constraints:	
Recommendation Justification:	Datafile is a java utility to read/write data from files in various formats. Datafile was written by a single developer, the last version released 4 years ago. The user base is probably very small and support for this utility is not available. For these reasons, it is not recommended for approval enterprise wide.

6.8) Dreamweaver

General Information

Website:	http://www.adobe.com/products/dreamweaver/
Description:	Dreamweaver is a web development application that incorporates support for Web technologies such as CSS, JavaScript, and various server side scripting languages and frameworks including ColdFusion, Java Server Pages (JSP) and PHP. Dreamweaver has a visual editing tool that is targeted at less experienced users but also includes tools and features for professional Web developers. Only projects with current ARB waivers should be using Dreamweaver. All others should take advantage of the Rational tools offered by the Enterprise Tools Management team.
Decision:	Prohibited
Decision Constraints:	
Decision Source:	ARB

Decision Process:	TRM v3
Decision Date:	1/7/2009
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	Adobe

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	867: Integrated Development Environments (IDE)

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Rational Software Architect
- Rational Systems Developer
- Rational Application Developer
- Rational Web Developer

General Analysis

Architectural Area

- Application

Architectural Benefits

- The use of Dreamweaver promotes the creation of rich, thin-client user interfaces for the presentation tier of HeV.

Architectural Risks

- The proliferation of multiple development tools in the enterprise may lead to silos of knowledge and skills that cannot move easily between projects.

Tier Used

- Presentation Tier

Tool Type

- Commercial

Tool Usage

- Management/Collaboration

General Assessment

Expected Usage:	Provides the ability to design, develop and maintain web based content.
Assessment Type:	New
Assessment Date:	11/17/2008
Notes:	As Adobe purchased Macromedia in 2005, industry analysts have predicted that (Macromedia's) Dreamweaver and (Adobe's) GoLive will have concurrent and parallel development for at least two more major releases, then one of the products will fold or be merged into the other. Evidence of this is the inclusion of GoLive into the latest release of Dreamweaver. Note that support for ASP .NET has been dropped from DS4 and that JSP support will be removed in CS4. Refer to: http://www.adobe.com/go/kb402489
Recommendation:	Deny
Recommendation Constraints:	
Recommendation Justification:	The recommendation is to use Dreamweaver only with a wavier in special circumstances. There are (currently) four tools in the Rational suite that have capabilities equal to Dreamweaver; Enterprise Tools Management has designated Eclipse-based Rational development environments as the standard. In addition, it has been announced that future versions of Dreamweaver will not support Java Server Pages (due to the Adobe acquisition of Macromedia).

6.9) Drools

General Information

Website:	http://www.jboss.org/drools/
Description:	Drools is an open source business rule management system and a rules engine for the Java language. **Note: JRules is the approved technology for business rules management.**
Decision:	Prohibited
Decision Constraints:	
Decision Source:	ARB
Decision Process:	TRM v3.2
Decision Date:	8/19/2009
Current Status:	Analysis Completed
Introduced By:	ARB
Vendor Name:	JBoss

FEA Categories

Service Area	Service Category	Service Standard Code
N/A	N/A	N/A

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- JRules Business Rules Management Server

- JRules Rule Execution Server

General Analysis

Adoption Benefits

- Drools would provide a low-cost alternative to JRules.

Adoption Risks

- Drools is targeted primarily at leading-edge open-source developers and releases may not be stable.

Architectural Benefits

- None significant.

Architectural Risks

- Drools does not support the use of the "else" logic statement, which may be challenging when writing rules. There are a number of reported cases where developers can implement rules that lead to an infinite loop.

General Assessment

Expected Usage:	Drools would be used to provide a Business Rules Management System for externalizing business rules which change frequently from VA applications.
Assessment Type:	New
Assessment Date:	6/23/2009
Notes:	Drools is a JBoss.org open source project developed in the open source community; as new features in Drools are developed, tested, and become stable in the community, JBoss brings them into the enterprise-ready, subscription-based product: JBoss Enterprise BRMS.
Recommendation:	Deny
Recommendation Constraints:	Note that Drools requires the use of the JBoss application server.
Recommendation Justification:	The VA currently has selected JRules Business Rules Management System (BRMS) to provide externalized business rules support for VA applications. This is a commercial BRMS, which encompasses all of the capabilities that Drools would provide and includes commercial support. For this reason there is

no need for a secondary technology to support business rules externalization.

6.10) GroboUtils

General Information

Website: http://groboutils.sourceforge.net/index.html

Description: GRoboUtils is a set of testing utilities implemented in Java. The utilities support multi-threaded and hierarchical unit testing and includes a code coverage analysis tool, and user interface recording feature to capture and playback UI interactions.
Note: The approved technologies for unit testing and code coverage are Junit and JProbe.

Decision: Prohibited

Decision Constraints:

Decision Source: ARB

Decision Process: TRM v4.1

Decision Date: 10/28/2009

Current Status: Analysis Completed

Introduced By: ARB

Vendor Name: N/A

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	869: Test Management

Operating Systems Supported

- Red Hat Linux
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- JUnit
- JProbe

General Analysis

Adoption Benefits

- Multi-threaded testing aids in the discovery of timing related software defects in multi-threaded implementations.

Adoption Risks

- GroboUtils is a set of utilities developed primarily by a single developer. It has not been updated in 5 years and no support is available.

Architectural Benefits

- None significant.

Architectural Risks

- None significant.

Tool Type

- Framework

General Assessment

Expected Usage:	GroboUtils is used primarily by software engineers for unit testing.
Assessment Type:	New
Assessment Date:	10/1/2009
Notes:	
Recommendation:	Deny
Recommendation Constraints:	
Recommendation Justification:	GroboUtils is a set of Java utilities supporting unit and functional testing developed primarily by a single software engineer. There have been no new releases published for 5 years and there is no

support available.

6.11) i-net JDBC Drivers

General Information

Website: http://www.inetsoftware.de/products/jdbc-driver

Description: JDBC type 4, platform-independent drivers for various databases including MS SQL Server, Oracle, Sybase, and DB2.
Note: The JDBC driver provided by the vendor for an approved RDBMS is the JDBC driver technology to be used.

Decision: Prohibited

Decision Constraints:

Decision Source: ARB

Decision Process: TRM v4

Decision Date: 9/16/2009

Current Status: Analysis Completed

Introduced By: ARB

Vendor Name: i-net software

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	Data Management	893: Database Connectivity

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Oracle JDBC Drivers
- Cache JDBC Driver

General Analysis

Adoption Benefits

- Improved performance
- Smaller footprint

Adoption Risks

- Multiple JDBC drivers for a target RDBMS may increase support costs

Standards Traceability

- SQL

General Assessment

Expected Usage:	The Oranxo verion of JDBC driver for Oracle is to be used for database access for CrystalClear as part of the Outpatient Appointment Scheduling application (RSA)
Assessment Type:	New
Assessment Date:	8/4/2009
Notes:	
Recommendation:	Deny
Recommendation Constraints:	
Recommendation Justification:	JDBC drivers are packaged and licensed with vendor databases. There are no real advantages to acquiring additional JDBC drivers to provide the same funtionality already provided by the RDBMS vendors JDBC driver. The database abstraction benefit identified by i-net is negated with the mandated use of Hibernate for object relational mapping (ORM).

6.12) Jakarta Object Relational Bridge

General Information

Website:	http://db.apache.org/ojb/
Description:	Jakarta Object Relational Bridge is now known as Apache ObJectRelationalBridge (OJB). OJB is an Object/Relational mapping tool that allows persistence for Java Objects against relational databases. **Note: Hibernate is the approved technology for object relational mapping.**
Decision:	Prohibited
Decision Constraints:	
Decision Source:	HSD&D
Decision Process:	ETL
Decision Date:	12/1/2006
Current Status:	Introduced
Introduced By:	Extended Tool List (ETL)
Vendor Name:	ASF

FEA Categories

Service Area	Service Category	Service Standard Code
N/A	N/A	N/A

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

General Analysis

ETL Prohibited Technology/Standard, TRM Analysis still pending.

General Assessment

ETL Prohibited Technology/Standard, TRM Assessment still pending.

6.13) JavaServer Faces Reference Implementation

General Information

Website: http://java.sun.com/javaee/javaserverfaces/

Description: Reference implementation of JavaServer Faces specification implemented as part of the Project Mojarra under Glassfish a reference implementation of the Java Enterprise Edition standards. JavaServer Faces provides a component based framework for constructing web-based user interfaces. The JavaServer Face specification is part of the Java Enterprise Edition standards. **Note: Apache Struts is the approved web user interface framework for application development.**

Decision: Prohibited

Decision Constraints:

Decision Source: HSD&D

Decision Process: ETL

Decision Date: 12/1/2006

Current Status: Introduced

Introduced By: Extended Tool List (ETL)

Vendor Name: Sun Microsystems

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	895: Middleware

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- Apache Struts

General Analysis

ETL Prohibited Technology/Standard, TRM Analysis still pending.

General Assessment

ETL Prohibited Technology/Standard, TRM Assessment still pending.

6.14) JBoss

General Information

Website:	http://www.jboss.com/products/platforms/application/?sc_cid=70160000000Hm0uAAC&s_kwcid=TC|4654|jboss||S|e|3346520121
Description:	JBoss is an open-source Java Enterprise Edition application server platform, designed to host distributed applications written using Java and the Java Enterprise Edition frameworks. **Note: Weblogic Server is the approved application server technology.**
Decision:	Prohibited
Decision Constraints:	
Decision Source:	HSD&D
Decision Process:	ETL
Decision Date:	12/1/2006
Current Status:	Introduced
Introduced By:	Extended Tool List (ETL)
Vendor Name:	RedHat

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Delivery Servers	873: Application Servers

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- WebLogic Server

General Analysis

ETL Prohibited Technology/Standard, TRM Analysis still pending.

General Assessment

ETL Prohibited Technology/Standard, TRM Assessment still pending.

6.15) jBPM

General Information

Website:	http://www.jboss.com/products/jbpm
Description:	JBoss Java Business Process Management (jBPM) is a framework that provides workflow, business process management (BPM), and process orchestration for the Java developer.
Decision:	Prohibited
Decision Constraints:	
Decision Source:	ARB
Decision Process:	TRM v4.1
Decision Date:	10/28/2009
Current Status:	Analysis Completed
Introduced By:	ARB
Vendor Name:	RedHat

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	895: Middleware

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- WebLogic Integration

General Analysis

Adoption Benefits

- JBoss jBPM would provide a low-cost alternative to WebLogic Integration and is a well know Business Process Management Framework.

Adoption Risks

- Weblogic Integrator already provides similar capabilities. Multiple companion technologies may present compatibility and portability issues.

Architectural Benefits

- JBoss jBPM does support the industry standard BPEL.

Architectural Risks

- JBoss jBPM duplicates functionality provided by Weblogic Integrator.
- JBoss jBPM is owned by JBoss which implements the JBoss Application Server which is prohibited. Though this may not be an issue, there could be potential dependency on JBoss Application Server in future releases.
- BPEL is portable provide vendor extensions are not leveraged. This presents a risk

when leveraging multiple tools that support BPEL, it is possible that a definition may not be portable.

General Assessment

Expected Usage:	Provide Business Process Management, workflow, service orchestration and web page navigation capabilities described using Business Process Execution and Java Process Definition Languages.
Assessment Type:	New
Assessment Date:	9/21/2009
Notes:	
Recommendation:	Deny
Recommendation Constraints:	
Recommendation Justification:	Adoption of jBPM would result in multiple technologies in this area and duplicate functionality. Weblogic Integrator currently provides BPM capabilities and is an approved technology within the TRM.

6.16) JDK - JRockit

General Information

Website:	http://www.oracle.com/technology/products/jrockit/index.html
Description:	The Oracle JRockit Java Development Kit (JDK) provides tools, utilities, and a complete runtime environment for developing and running applications using the Java programming language. The JRockit JDK includes the Oracle JRockit JVM implementation of the Java runtime environment (JRE).
Decision:	Prohibited
Decision Constraints:	
Decision Source:	ARB
Decision Process:	TRM v3
Decision Date:	1/7/2009

Current Status: Analysis Completed
Introduced By: Extended Tool List (ETL)
Vendor Name: Oracle

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- JDK - HP-UX Java Development Kit
- JDK - IBM Java Software Developer Kit
- JDK - Sun Java SE Development Kit

General Analysis

Adoption Risks

- Potential use of vendor specific libraries may result in Java application code that is not 100% pure Java and portable to other Java Enterprise Edition application servers. This could result in BEA WebLogic vendor lock-in.

Architectural Benefits

- JRockit provides a specialized JVM tuned for the WebLogic Server that could eliminate some issues and improve performance for some applications.
- Bytecode generated by the JRockit JDK may be optimized to run on specific hardware and take advantage of operating system and WebLogic optimizations.

Architectural Risks

- Vendor JDK may lag behind current release of the Java SE standard.

- Bytecode generated by the JRockit JDK and optimized for JRockit JRE may lead to performance based vendor lock-in and could lead to code that is less portable.
- Unnecessary introduction of another Java Development Kit in the enterprise may complicate application development. Developers will need to learn both the Sun JDK based Java Standard Edition--and the JRockit SDK along with any deviations from the standard.

General Assessment

Expected Usage:	Compile, build, and execute Java applications optimized for BEA WebLogic. Applications will be executed with the JRockit JRE.
Assessment Type:	Refresh
Assessment Date:	11/17/2009
Notes:	
Recommendation:	Deny
Recommendation Constraints:	
Recommendation Justification:	The VA currently has approved Java Development Kit (JDK) and Java Runtime Environments (JRE) that support development, compilation, and execution of Java code on all supported platforms. The benefits of introducing a specialized JDK and the associated JRE do not offset the complexity, in both development and maintenance, which would be introduced with JRockit. Therefore it is recommended that JRockit be prohibited.

6.17) JRE - JRockit

General Information

Website:	http://www.oracle.com/technology/products/jrockit/index.html
Description:	Formerly known as BEA JRockit. JRockit is a specialized Java runtime environment (JRE) tuned specifically for WebLogic Server. The JRockit JVM implementation of the Java runtime environment includes the JRockit JVM, class libraries, and other files that support the execution of programs written in Java.
Decision:	Prohibited
Decision Constraints:	

Decision Source:	ARB
Decision Process:	TRM v3
Decision Date:	1/7/2009
Current Status:	Analysis Completed
Introduced By:	Extended Tool List (ETL)
Vendor Name:	Oracle

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Support Platform	865: Independent Platform

Operating Systems Supported

- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Websphere Application Server - ***(required for some configurations)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

General Analysis

Architectural Area

- Application

Architectural Benefits

- A specialized JVM tuned for the WebLogic Server could eliminate memory leaks and improve performance for some applications.

Architectural Risks

- The introduction of another Java Runtime Environment (JRE) into environments that already support the Sun JRE or a platform specific JRE will complicate support and

maintenance. Having another layer of Java Virtual Machine complexity will make application upgrades more difficult.

Tier Used

- All

Tool Usage

- Runtime

General Assessment

Expected Usage:	Customized Java Runtime Environment (JRE) for execution of Java applications built for the WebLogic Server.
Assessment Type:	New
Assessment Date:	10/20/2008
Notes:	When the BEA contract was approved, the primary reason was to gain the WebLogic application server. However, the contract bundled other BEA products, such as JRockit. JRockit was listed as "Prohibited" in the Extended Tools List.
Recommendation:	Deny
Recommendation Constraints:	
Recommendation Justification:	The introduction of another Java Runtime Environment (JRE) into environments that already support the Sun JRE or a platform specific JRE will increase the support and maintenance complexity while providing minimal benefits. There for it is recommended that JRockit JRE be prohibited in favor of the Sun JRE or a required platform specific JRE.

6.18) M2Eclipse

General Information

Website:	http://m2eclipse.sonatype.org/
Description:	Maven Integration for Eclipse provides integration for Maven into the Eclipse IDE **Note: Rational Build Forge is the approved software build technology.**

Decision:	Prohibited
Decision Constraints:	
Decision Source:	ARB
Decision Process:	TRM v4.1
Decision Date:	10/28/2009
Current Status:	Analysis Completed
Introduced By:	ARB
Vendor Name:	N/A

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	868: Software Configuration Management

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***
- Eclipse - ***(required libraries)***
- Maven - ***(required libraries)***

Comparable Technologies/Standards:

- Rational Build Forge

General Analysis

Tool Type

- Refer to Maven for analysis details

General Assessment

Expected Usage:	
Assessment Type:	New
Assessment Date:	9/18/2009
Notes:	Refer to the Maven assessment for additional details
Recommendation:	Deny
Recommendation Constraints:	
Recommendation Justification:	Maven is a prohibited technology

6.19) Maven

General Information

Website:	http://maven.apache.org/index.html
Description:	Maven is a software build tool that provides object structure and organization to facilitate the sharing of build logic across projects. The reusability aspect is viewed as an improvement compared to the ANT build tool. However, Maven should not be viewed as the next generation of ANT--as they have different architectures. Maven maintains project attributes of dependencies, artifacts, reports, remote and local repositories in a project object model. **Note: Rational Build Forge is the approved software build technology.**
Decision:	Prohibited
Decision Constraints:	
Decision Source:	ARB
Decision Process:	TRM v3
Decision Date:	1/7/2009
Current Status:	Analysis Completed
Introduced By:	TRM Team

Vendor Name: ASF

FEA Categories

Service Area	Service Category	Service Standard Code
Entry not classified		

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- ANT
- Rational Build Forge

General Analysis

Architectural Area

- Application

Architectural Benefits

- The directory structure imposed by Maven could bring standardization in the form of a consistent organization of software libraries.

Architectural Risks

- Maven lacks access control and auditing functionality found in commercial tools--significant in a health care environment.
- The proliferation of multiple build tools in the enterprise may lead to silos of knowledge and skills that cannot move easily between projects. For example, Maven requires a specific directory structure that may be incompatible with projects not using Maven.

Tier Used

- Integration Tier

Tool Type

- Open Source

Tool Usage

- Development

General Assessment

Expected Usage:	Java project organization and build tool.
Assessment Type:	New
Assessment Date:	11/13/2008
Notes:	ARB waivers that have been granted for the use of Maven: • 08-081 DTK use of Maven 2 • 08-062 CISS use of Maven • 08-052 MHV use of Maven 2 • 08-045 HDR II Maven Integration • 08-043 HDR II Maven
Recommendation:	Deny
Recommendation Constraints:	
Recommendation Justification:	Open source build systems (Maven, Cruise Control, ANT) come from and are driven by the needs of software developers. However, the development viewpoint can be myopic--limited to a specialized task with one concern: a successful build. This limited view of the enterprise is not usually concerned with compliance, access controls, functional-physical configuration accounting and reporting. Rational Build Forge has been identified as the OED standard software build tool by the Enterprise Tools Management team. Build Forge can perform software builds, do continuous integration, release builds (branches), and provides functionality for audits and role-based access to elements of the build. Build Forge is distinguished from open source tools in that it can control access to objects that compose the build. In Build Forge, each object has permission attributes. That means it is possible to hide sensitive information, (such as a password setting) and restrict access to that attribute for a specific user or group.

Also, Build Forge has capabilities to securely accommodate the mix of software created by the VA and by external contractors. For example, with Build Forge it's possible to limit the access of contractors to certain parts of the build. As a member of the Rational suite, Build Forge has a tight integration with ClearCase and ClearQuest.

Another differentiator for Build Forge is its agent-based method of creating build farms. While other build systems can distribute the build process, Build Forge is unique with its combination of access controls, workflow based builds, and the distribution of build agents. This approach allows for increased performance, but more importantly, can create a "native build". For example, a team that works on Windows for development can send the build to a Red Hat server for compilation in the destination operating environment.

So while Build Forge may not be as familiar to developers as Maven (Build Forge is not free), when viewed from the enterprise perspective it has distinct advantages over open source tools. The recommendation is to allow the use of Maven only when specific circumstances warrant an exception.

6.20) MediaWiki

General Information

Website:	http://www.mediawiki.org
Description:	MediaWiki is an open source Wiki platform that support collaborative development of web content using a simple markup language and editor that can be used from any web browser. MediaWiki is written in PHP and was originally develop for use on Wikipedia to replace UseModWiki a Perl based Wiki software platform. **Note: TeamPage is the approved collaborative web content development platform.**
Decision:	Prohibited
Decision Constraints:	
Decision Source:	ARB
Decision Process:	TRM v3.2

Decision Date: 8/19/2009
Current Status: Analysis Completed
Introduced By: TRM Team
Vendor Name: Wikimedia Foundation, Inc.

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Access Channels	852: Collaboration / Communications

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- MySQL - ***(required libraries)***
- Internet Information Services (IIS) - ***(required libraries)***
- Apache HTTP Server - ***(required libraries)***

Comparable Technologies/Standards:

- TeamPage

General Analysis

Adoption Benefits

- Adoption of MediaWiki would provide a platform for developing and publishing collaborative content.

Adoption Risks

- Adoption would require knowledge of how to install and customize MediaWiki to work with Oracle or SQL Server.
- Adoption would potentially require the VA to acquire specialized skills in PHP software development and support.

Architectural Benefits

- MediaWiki has a stable architecture and a proven track record supporting Wikipedia one of the oldest and best known Wiki sites in the industry.

Architectural Risks

- MediaWiki depends on an open source database such as MySQL, PostgreSQL, Ingres or SQLite. MySQL is a prohibited technology and the others have not been assessed at this time. Though MediaWiki will work with Microsoft SQL Server, it will not do so out of the box.
- MediaWiki depends on PHP which is a dynamic scripting language used to enable development of dynamic content similar to ASP and JSP. PHP has not been requested or assessed at this time. The proliferation of multiple development tools in the enterprise may lead to silos of knowledge and skills that cannot move easily between projects.

General Assessment

Expected Usage:	Provide a platform collaborative development of web content which can benefit the VA.
Assessment Type:	New
Assessment Date:	5/20/2009
Notes:	
Recommendation:	Deny
Recommendation Constraints:	
Recommendation Justification:	MediaWiki depends on an open source database such as MySQL, PostgreSQL, Ingres or SQLite, though it will run on Microsoft SQL Server, it will not run out of the box. MySQL is a prohibited technology and PostgreSQL, Ingres and SQLite have never been assessed. MediaWiki also depends on PHP which is another web development language similar to ASP and JSP for developing dynamic content. PHP has not been assessed. Though MediaWiki is a widely adopted Wiki software platform like many other Wiki platforms it depends on languages and databases that do not align with VA chosen technologies and standards. For this reason MediaWiki should be prohibited.

6.21) MetaHelper

General Information

Website: http://sourceforge.net/projects/metahelper/

Description: Metahelper is a tool designed to automate the operations required for configuration metapackage administration. Specifically, Metahelper manages the addition, subtraction, and merging of system configuration change-sets (deltas) on a per delta bases. Allowing for multiple deltas to affect the contents of the same files in a transitive, and reversible way.

Decision: Prohibited

Decision Constraints:

Decision Source: ARB

Decision Process: TRM v4

Decision Date: 9/16/2009

Current Status: Analysis Completed

Introduced By: ARB

Vendor Name: N/A

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	868: Software Configuration Management

Operating Systems Supported

- Red Hat Linux

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

General Analysis

Adoption Risks

- Immature product
- No documented support
- Very low market penetration
- No product documentation

Architectural Benefits

- Automated configuration metapackage administration

General Assessment

Expected Usage:	Deployment Toolkit (DTK) will utilize this technology in the support of application and hardware configurations
Assessment Type:	New
Assessment Date:	8/6/2009
Notes:	
Recommendation:	Deny
Recommendation Constraints:	
Recommendation Justification:	This is an immature, unsupported, sparsely utilized technology. SourceForge seems to be the only location for information regarding this technology and the documentation is non-existent. There is no documented support contact. The only posting of source code (v0.89) was on 2/13/08. On the date of this assessment there were only 21 downloads indicated.

6.22) MySQL

General Information

Website:	http://www.mysql.com/
Description:	MySQL is an open-source relational database management system (RDBMS) **Note: Oracle Database, SQL Server, and Cache are the approved database technologies. Refer to each of these entries for any specific constraints regarding their use.**
Decision:	Prohibited
Decision Constraints:	

Decision Source:	HSD&D
Decision Process:	ETL
Decision Date:	12/1/2006
Current Status:	Introduced
Introduced By:	Extended Tool List (ETL)
Vendor Name:	Sun Microsystems

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Database/Storage	875: Database

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Cache Database Engine
- Oracle Database
- SQL Server

General Analysis

ETL Prohibited Technology/Standard, TRM Analysis still pending.

General Assessment

ETL Prohibited Technology/Standard, TRM Assessment still pending.

6.23) Oracle Data Service Integrator

General Information

Website: http://download.oracle.com/docs/cd/E13162_01/odsi/docs10gr3/index.html

Description: Oracle Data Service Integrator, formerly know as AquaLogic Data Services Platform and BEA WebLogic Liquid Data, provides real-time aggregation of information across hetergeneneous data sources through the use of data services. Data services encapsulate the logic for reading, writing, and transforming information, insulating data consumers from having to contend with multiple data source formats and connection mechanisms.

Decision: Prohibited

Decision Constraints:

Decision Source: HSD&D

Decision Process: ETL

Decision Date: 12/1/2006

Current Status: Introduced

Introduced By: Extended Tool List (ETL)

Vendor Name: Oracle

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	895: Middleware

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

General Analysis

ETL Prohibited Technology/Standard, TRM Analysis still pending.

General Assessment

ETL Prohibited Technology/Standard, TRM Assessment still pending.

6.24) PDF Renderer

General Information

Website: https://pdf-renderer.dev.java.net/

Description: PDF Renderer is an open source, all Java library which renders PDF documents to the screen using Java2D.

Decision: Prohibited

Decision Constraints:

Decision Source: ARB

Decision Process: TRM v4.1

Decision Date: 10/28/2009

Current Status: Analysis Completed

Introduced By: ARB

Vendor Name: N/A

FEA Categories

Service Area	Service Category	Service Standard Code
Component Framework	User Presentation/Interface	887: Dynamic Server-Side Display
Component Framework	User Presentation/Interface	888: Content Rendering
Service Interface and Integration	Integration	895: Middleware

Operating Systems Supported

- AIX
- HP-UX

- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

General Analysis

Adoption Benefits

- High performance PDF document printing capability
- LGPL license

Adoption Risks

- Only supports a subset 1.4 of the PDF specification. The latest PDF specification is 1.7. It does not support transparency, various font encodings or fill-in forms.
- Limited developer only support
- Immature technology. Only one version released.

General Assessment

Expected Usage:	PDF file viewing and printing
Assessment Type:	New
Assessment Date:	10/5/2009
Notes:	Analysis needs to be performed on comparable technologies such as Adobe Reader, jPDF, jPedal, and jPDFPrint
Recommendation:	Deny
Recommendation Constraints:	
Recommendation	This technology is currently immature with a very small user base.

Justification:

6.25) Perforce

General Information

Website: http://www.perforce.com/

Description: Perforce is a software configuration management system. **Note: Rational ClearCase with Multisite and Rational Team Concert are the approved technologies for software configuration management.**

Decision: Prohibited

Decision Constraints:

Decision Source: HSD&D

Decision Process: ETL

Decision Date: 12/1/2006

Current Status: Introduced

Introduced By: Extended Tool List (ETL)

Vendor Name: Perforce Software

FEA Categories

Service Area	Service Category	Service Standard Code
N/A	N/A	N/A

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Rational ClearCase with MultiSite
- Rational Team Concert

General Analysis

ETL Prohibited Technology/Standard, TRM Analysis still pending.

General Assessment

ETL Prohibited Technology/Standard, TRM Assessment still pending.

6.26) Rational XDE Developer

General Information

Website:	http://www.ibm.com/software/rational/
Description:	Rational XDE Developer is a design and development environment for Java and .NET platforms. **Note: Vendor support for this product was discontinued on 6/5/2006. Approved technologies for design and development are Rational Software Architect, Rational Software Modeler, and Eclipse.**
Decision:	Prohibited
Decision Constraints:	Contact the Software Engineering Tools Management Division for details on the constraints for use of this technology.
Decision Source:	HSD&D
Decision Process:	ETL
Decision Date:	12/1/2006
Current Status:	Introduced
Introduced By:	Extended Tool List (ETL)
Vendor Name:	IBM

FEA Categories

Service Area	Service Category	Service Standard Code

Service Platform and Infrastructure	Software Engineering	867: Integrated Development Environments (IDE)

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Rational Application Developer

General Analysis

ETL Prohibited Technology/Standard, TRM Analysis still pending.

General Assessment

ETL Prohibited Technology/Standard, TRM Assessment still pending.

6.27) Rational XDE Tester

General Information

Website:	http://www.ibm.com/software/rational/
Description:	Rational XDE Tester is an automated testing framework that provides functional, regression, GUI, and data-driven testing capabilities. **Note: Vendor support for Rational XDE Tester was discontinued on 4/30/2008. The approved technology for functional regression testing is Rational Functional Tester.**
Decision:	Prohibited
Decision Constraints:	Contact the Software Engineering Tools Management Division for details on the constraints for use of this technology.
Decision Source:	HSD&D
Decision	ETL

Process:
Decision Date: 12/1/2006
Current Status: Introduced
Introduced By: Extended Tool List (ETL)
Vendor Name: IBM

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	869: Test Management

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- Rational Functional Tester

General Analysis

ETL Prohibited Technology/Standard, TRM Analysis still pending.

General Assessment

ETL Prohibited Technology/Standard, TRM Assessment still pending.

6.28) TestNG

General Information

Website: http://testng.org/doc/index.html
Description: TestNG is an open source testing framework designed to automate unit, functional, end-to-end, integration and other forms of testing scenarios.
Note: The approved technologies for functional testing are

Rational Functional Tester, Rational Manual Tester, and JUnit.

Decision: Prohibited

Decision Constraints:

Decision Source: ARB

Decision Process: TRM v4

Decision Date: 9/16/2009

Current Status: Analysis Completed

Introduced By: Extended Tool List (ETL)

Vendor Name: TestNG

FEA Categories

Service Area	Service Category	Service Standard Code
Service Platform and Infrastructure	Software Engineering	869: Test Management

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- JRE - Sun - ***(required libraries)***

Comparable Technologies/Standards:

- JUnit
- Rational Functional Tester
- Rational Manual Tester

General Analysis

Adoption Benefits

- Test Driven Development helps insure early detection of potential problems allowing

them to be resolved early in the SDLC where the cost is lower. This leads to greater application and architecture stability.

Adoption Risks

- Having overlapping testing framework TestNG and Junit/Rational may reduce testing portability and increase support costs.

Architectural Benefits

- TestNG extends beyond unit testing, providing an open source framework and alternative to commercial products in the area of functional, end-to-end, integration and other more complex testing.
- TestNG provide a plug-in for IDE integration that encompasses the IDEs approved in the TRM.

Architectural Risks

- TestNG does not add any additional benefits currently provided by JUnit and the Rational Testing Tools. Too many overlapping testing frameworks may impact standardized VA testing capabilities.
- Though TestNG provides a plug-in for most IDEs it currently does not provide automated test generation that exists with the JUnit plug-in. This auto test generation simplifies creation of unit tests within the developers IDE. This capability may be included in the future.

Tool Type

- Framework

Tool Usage

- TestNG is used for unit, end-to-end, integration and other forms of testing.

General Assessment

Expected Usage:	Framework to support Test Driven Development activities and automate unit testing.
Assessment Type:	New
Assessment Date:	8/7/2009
Notes:	TestNG has gained traction since its introduction in 2004 and is steadily growing in popularity. Its popularity has resulted in improvements in JUnit. It recommended that the VA continue to monitor both Junit and TestNG continually re-evaluating which is the most appropriate framework for developer testing.

Recommendation:	Deny
Recommendation Constraints:	
Recommendation Justification:	Though TestNG is an emerging open source testing framework for unit, functional, end-to-end, integration and other forms of testing, this space is already covered by JUnit and the Rational Testing Tools and does not warrant another testing framework at this time. Additionally JUnit comes bundled with most IDEs and is readily available to developers and is well integrated. TestNG is a plug-in that requires download, installation and configuration.

6.29) TPTP

General Information

Website:	http://www.eclipse.org/tptp/
Description:	The Test and Performance Tools Platform Project (TPTP) is a set of testing frameworks that provides the ability to develop testing capabilities, i.e. unit and functional testing tools, tracing and profiling tools for memory and performance analysis, and monitoring tools used to build application and system monitoring and logging facilities. **Note: The approved technologies for testing are Rational Functional Tester, Rational Manual Tester, Rational Performance Tester, Rational PurifyPlus, and Junit.**
Decision:	Prohibited
Decision Constraints:	
Decision Source:	ARB
Decision Process:	TRM v4.1
Decision Date:	10/28/2009
Current Status:	Analysis Completed
Introduced By:	ARB
Vendor Name:	Eclipse

FEA Categories

Service Area	Service Category	Service Standard Code

Operating Systems Supported

- Red Hat Linux
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Eclipse - ***(required libraries)***

Comparable Technologies/Standards:

- Rational TestManager
- Rational Functional Tester
- Rational Manual Tester
- Rational Performance Tester
- Mercury LoadRunner
- Mercury WinRunner
- Rational PurifyPlus

General Analysis

Adoption Benefits

- Adoption of this technology will not increase the current benefits provided by Rational Functional Tester, Rational Performance Tester, and Rational PurifyPlus.

Adoption Risks

- Adopting mutiple comparable technologies increases support costs (training, maintenance, etc.)

Architectural Benefits

- TPTP provides open source frameworks that are interoperable and integrated with Eclipse platform tools.

Architectural Risks

- Nothing significant

Tool Type

- Framework

General Assessment

Expected Usage:	TPTP supports full range of testing including unit testing, functional testing as well as performance monitoring and profiling.
Assessment Type:	New
Assessment Date:	9/23/2009
Notes:	Although this technology is packaged with one or more approved technologies, its stand alone use is not permitted as it duplicates the functionality provided by an existing approved technology.
Recommendation:	Deny
Recommendation Constraints:	
Recommendation Justification:	While TPTP is a mature set of open source frameworks supporting the development of unit and functional testing tools, profiling and logging capabilities and performance monitoring, the Rational suite of testing tools, along with Junit, provide similar testing capabilities.

6.30) Tuxedo

General Information

Website:	http://www.oracle.com/technology/products/tuxedo/index.html
Description:	Tuxedo, formerly known as BEA WebLogic Tuxedo, provides the framework, or middleware, for building scalable multi-tier client/server applications in heterogeneous (dissimilar), distributed environments. Tuxedo provides a service-oriented infrastructure for routing, dispatching, and managing requests, events, and application queues across system processes and application services.
Decision:	Prohibited
Decision Constraints:	
Decision Source:	HSD&D
Decision Process:	ETL

Decision Date: 12/1/2006
Current Status: Introduced
Introduced By: Extended Tool List (ETL)
Vendor Name: Oracle

FEA Categories

Service Area	Service Category	Service Standard Code
Service Interface and Integration	Integration	895: Middleware

Operating Systems Supported

- Operating Systems Platforms have not been specified.

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified at this time.

Comparable Technologies/Standards:

- No comparable products have been identified at this time.

General Analysis

ETL Prohibited Technology/Standard, TRM Analysis still pending.

General Assessment

ETL Prohibited Technology/Standard, TRM Assessment still pending.

6.31) TWiki

General Information

Website: http://www.twiki.org
Description: TWiki is an open source Wiki platform providing enterprise users the ability to collaboratively develop web content. It is a Structured Wiki or a Wiki that incorporates database technology. The TWiki is typically used in collaborative efforts where the goal is to develop and publish content. The TWiki is built on Perl and provides a plug-in architecture for contributed additional functionality.

	Note: Teampage is the approved collaborative web content development platform.
Decision:	Prohibited
Decision Constraints:	
Decision Source:	ARB
Decision Process:	TRM v3.2
Decision Date:	8/19/2009
Current Status:	Introduced
Introduced By:	TRM Team
Vendor Name:	Twiki.net

FEA Categories

Service Area	Service Category	Service Standard Code
Service Access and Delivery	Access Channels	852: Collaboration / Communications

Operating Systems Supported

- AIX
- HP-UX
- Red Hat Linux
- Solaris
- Windows (Client)
- Windows (Server)

Technologies/Standards Relationships

Runtime Dependencies:

- Apache HTTP Server - ***(required libraries)***
- Perl - ***(required libraries)***

Comparable Technologies/Standards:

- TeamPage

General Analysis

Architectural Benefits

- TWiki plug-in architecture does allow for addition of capabilities based on need. It also

allows the TWiki platform to be customized based on the planned usage.
- TWiki is a widely used and supported Wiki software product and has been used by Disney, Yahoo and SAP. Although the primary use has been document management, software development and project collaboration.

Architectural Risks

- TWiki is based on Perl, which means that Perl skills will be required.
- TWiki depends on many UNIX/Linux commands such as RCS, diff, fgrep, grep and CRON. Though it will run on Windows you lose some functionality and it is considered an exceptional case.
- The Twiki plug-in architecture is powerful, but there are compatibility issues between plug-ins and the specific version of the Twiki. Plug-ins if overused can become a burden to manage.
- Twiki leverages flat files and the UNIX/Linux native Revision Control System (RCS) to store content and maintain a version history. This is unlike most Wiki software products which use a relational database. This could present a challenge over time.

Tier Used

- Presentation
- Middle Tier

Tool Type

- Content Management and Delivery

Tool Usage

- Online collaboration and content delivery

General Assessment

Expected Usage:	The TWiki is intended to be used to collaborate and publish EA Technical Reference Model (TRM) content. It will be used to allow VA organizations to author and comment on TRM content about technology or standards approved or prohibited within the VA.
Assessment Type:	New
Assessment Date:	6/24/2009
Notes:	The TWiki was not officially requested.
Recommendation:	Deny
Recommendation Constraints:	Limited to EA TRM use any other use should require a waiver and should be strongly discouraged.

Recommendation Justification: The EA TRM is currently implemented using TWiki software as such there is some investment in this product, which should not be discarded. However, future use of this technology should be prohibited. Though Perl knowledge is not required for basic use, any use of plug-ins or configuration issues will require an individual with Perl skills.

The Twiki can technically run on any platform however it has been targeted at UNIX/Linux machines. The Twiki leverages key UNIX/Linux technologies such as grep, RCS, diff, patch and cron. Deployment to Windows platforms can be challenging.

The plug-in architecture which allows for add-on functionality is a very powerful feature; however plug-in compatibility remains an issue with the Twiki. Some plug-ins only works with a specific version of the Twiki and some do not work at all without perl or perl framework knowledge such as knowledge of the Perl DBI database framework.

Unlike most Wiki software products storage and versioning of content is not based on database technology, but is based on the UNIX/Linux Resource Control System which is a file based storage and version control system.

A complete comparative analysis of Wiki software technologies should be considered and the most appropriate wiki software platform based on skill, operational environment and need should be selected.

7. Enterprise Infrastructure & Engineering Standard

7.1) Enterprise Engineering IT Infrastructure LAN Standard v1.0

7.2) Enterprise Engineering IT Infrastructure WAN Standard v1.0

7.3) Enterprise Engineering Enterprise Server Standard v1.0

7.4) Enterprise Engineering Enterprise Storage Standard v1.0

7.5) Enterprise Engineering Data Center Standard v1.0

DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INFORMATION AND TECHNOLOGY

ENTERPRISE INFRASTRUCTURE ENGINEERING

VA Enterprise IT Infrastructure Standard

Local Area Network

Production 1.0

November 5, 2009

TABLE OF CONTENTS

1 Introduction 1

1.1 Purpose 1

1.2 Objectives 1

1.3 Scope 1

2 Standards 2

2.1 CORE Network Switch 2

2.2 End-of-Row Access Layer Switch (10/100/1000 host connectivity) 4

2.3 High-Bandwidth Converged I/O Access Layer Switch (10GE Host connectivity) 6

2.4 VistA Private SCS DCI Router/Switch - 10MBPS 8

2.5 Blade Sever Chassis Access Layer Switch (10/100/1000 host connectivity) 10

2.6 Management Access Layer Switch 12

2.7 Load Balancer 14

3 Supporting Details for Standards 15

3.1 CORE Network Switch 15

3.1.1 Chassis 16

3.1.2 Packet Processor 19

3.1.3 Linecards/port interfaces 20

3.1.4 Operating System 22

3.1.5 Support 24

3.1.6 High Availability 25

3.2 End-of-Row Access Layer Switch (10/100/1000 host connectivity) 26

3.2.1 Chassis 26

3.2.2 Packet Processor 28

3.2.3 Linecards / Port Interfaces 29

3.2.4 Operating System 31
3.2.5 Support 32
3.2.6 High Availability 32
3.3 High-Bandwidth Converged I/O Access Layer Switch (10GE Host connectivity) 34
3.3.1 Chassis 34
3.3.2 Packet Processor 36
3.3.3 Linecards/port interfaces 38
3.3.4 Operating System 40
3.3.5 Support 42
3.3.6 High Availability 43
3.4 VistA Private SCS DCI Router/SWITCH - 10MBPS 43
3.4.1 Chassis 44
3.4.2 Packet Processor 46
3.4.3 Linecards/port interfaces 48
3.4.4 Operating System 50
3.4.5 Support 52
3.4.6 High Availability 53
3.5 Blade Sever Chassis Access Layer Switch 54
3.5.1 Chassis 54
3.5.2 Packet Processor 56
3.5.3 Interfaces 58
3.5.4 operating system 60
3.5.5 Support 62
3.5.6 High Availability 63
3.6 Management Access Layer Switch 64
3.6.1 Chassis 64
3.6.2 Packet Processor 65

3.6.3 Port Interfaces 66

3.6.4 Operating System 67

3.6.5 Support 68

3.6.6 High Availability 69

3.7 Load Balancer 71

4 Taxonomy of Standards 72

Appendix A – Definitions 75

Appendix B – References 75

Appendix C – Acronyms 75

Appendix D – Contributors 75

1 INTRODUCTION

1.1 PURPOSE

A standard is a set of rules or requirements that are determined by a consensus opinion of subject matter experts and prescribe criteria for a product, process, test or procedure. The general benefits of a standard are quality, interchangeability of parts or systems, and consistency. Information Technology (IT) standards are based on business needs provided through or supported by IT Services. IT Services are designed to support business processes and are constructed from software, hardware and infrastructure components. Establishing and enforcing standards for the selection and configuration of these supporting components improves the maintainability, reliability and availability of IT Services within projected economic constraints in alignment with business needs.

This standards document lists the acceptable and recommended specifications for Local Area Network. Sections include standard specifications for subject components, decisions supporting the standard specifications, guidelines or recommendations for implementing the standard specifications, and supplemental factors to consider when evaluating subject components. Other supplementary documents will provide guidance on procuring components that meet the standard specifications, guidance on integrating them with existing components, and explanation of how the subject components fit into the VA Architecture.

1.2 OBJECTIVES

This standard provides acceptable and recommended specifications to support:

- Solution Evaluation
- Requirement Evaluation
- Solution Design
- Solution Procurement and Bid Evaluation
- Evaluation of Architectural Specifications
- Click here to enter a list of objectives specific to this standard.

1.3 SCOPE

This standard applies to:

- This standard applies to the Region 2 and Region 3 Data Center Local Area Network

2 STANDARDS

2.1 CORE NETWORK SWITCH

This specification set identifies the requirements for a core layer switch.

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
1	Chassis	Type	Modular
		Rack Mounting	Required
		System Throughput	>= 1.44 Tbps
		Packet Processor Redundancy Support	Preferred, (See Implementation Guidance)
		Control Plane Redundancy Support	Required
		Front-Back Airflow Support	Required
		Cooling Redundancy Support	Required
		Power Supply Redundancy Support	Required
		Online Insertion/Removable Hot-Pluggable	Required
2	Packet Processor	Type	Modular/Upgradable
		Layer 3 Switching Throughput (pps)	>= 450 Mpps
		Layer 2 Switching Throughput (pps)	>= 450 Mpps
		Online Insertion/Removal Support	Required
		Memory	>= 1 GB
		L3 Protocols switched in hardware	Required: IPv4, IPv6, MPLS / Preferred: GRE, NAT

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
3	Linecards/Port Interfaces	Interface Speed	10 Gigabit Ethernet and 1 Gigabit Ethernet
		Media Flexibility Support	MMF >= 26m, SMF >= 10km, SMF >= 40km, MMF >= 300m, MMF(850nm)-10GBASE-S, SMF(1310nm)-10GBASE-L, SMF(1550nm)-10GBASE-E, MMF/SMF-10GBASE-LX4, 10GBase-T(Cat6a)
		Port per ASIC (Oversubscription)	1:1 Preferred
		Throughput to Backplane	>= 40 Gbps
		Queuing Properties	200MB/port w/ Shaped Round Robin + DSCP Support TX: Priority: Preferred, Standard: >= 4 RX: Standard: >= 4
		Online Insertion/Removable Support	Required
		On-Card distributed packet forwarding support	Preferred
4	Operating System	Type	Non-Monolithic (Modular) Preferred
		Features Supported	802.1p, 802.1q, Broadcast Storm Control
		Multi-chassis Link Aggregation Support	Required
		Multi-chassis Management Interface Aggregation	Preferred
		Protocols Supported	Required: Link-Layer Discover Protocol, OSPF, BFD / Preferred: CDP, EIGRP
		Network Management	Centralized AAA w/ Role Based Authorization, Syslog SNMP v2c, v3 preferred
5	Support	Technical Support	24x7 Telephone/Web with customer option to immediately escalate to a senior engineer in a “network down” scenario.
		Parts Replacement	<= 24 hours, preferred <= 4 hours
6	High Availability	Operating System Maturity	Preferred released and QA Tested for >= 6 Months

ID	Primary Attribute	Secondary Attribute	Specification
		Hardware Maturity	Available for purchase for >= 3 Years
		Quality Assurance Certification	Employs a rigorous testing program in a laboratory environment that simulates a “real world” enterprise network. Testing of both hardware and software that verifies feature functionality and interoperability under “real world” traffic loads.

2.2 END-OF-ROW ACCESS LAYER SWITCH (10/100/1000 HOST CONNECTIVITY)

ID	Primary Attribute	Secondary Attribute	Specification
1	Chassis	Type	Modular (Multi-Slot)
		Rack Mounting	Required
		System Throughput	>=720 Mbps
		Packet Processor Redundancy Support	Required
		Control Plane Redundancy Support	Required
		Front-Back Airflow Support	Required
		Cooling Redundancy Support	Required
		Power Supply Redundancy Support	Required
		Online Insertion/Removable Hot-Pluggable	Required
2	Packet Processor	Type	Modular/Upgradable
		Layer 3 Switching Throughput (pps)	>= 450 Mpps
		Layer 2 Switching Throughput (pps)	>= 450 Mpps

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
		Online Insertion/Removable Support	Required
		Memory	>= 1 GB
		Protocols switched in hardware	IPv4, IPv6, MPLS, GRE, NAT (hardware-assisted)
3	Linecards/Port Interfaces	Interface Speed	10/100 Megabit Ethernet , 1 Gigabit Ethernet & 10 Gigabit Ethernet
		Media Flexibility Support	MMF >= 220m, SMF >= 10km, UTP Cat-5 MMF(850nm)-10GBASE-S, SMF(1310nm)-10GBASE-L, SMF(1550nm)-10GBASE-E, MMF/SMF-10GBASE-LX4
		Port per ASIC (Oversubscription	1:1 Preferred
		Throughput to Backplane	>= 40 Gbps
		Queuing Properties	TX: Priority: Preferred, Standard: >= 4 RX: Standard: >= 4
		Online Insertion/Removable Support	Required
		On-Card distributed packet forwarding support	Preferred
4	Operating System	Type	Non-Monolithic (Modular) Preferred
		Features Supported	802.1p, 802.1q, Broadcast Storm Control
		Multi-chassis Link Aggregation Support	Required
		Multi-chassis Management Interface Aggregation Support	Preferred
		Protocols Supported	Required: Link-Layer Discover Protocol, OSPF, BFD / Preferred: CDP, EIGRP
		Network Management	Centralized AAA w/ Role Based Authorization, Syslog SNMP v2c, v3 preferred

ID	Primary Attribute	Secondary Attribute	Specification
5	Support	Technical Support	24x7 Telephone/Web with customer option to immediately escalate to a senior engineer in a “network down” scenario.
		Parts Replacement	<= 24 hours, preferred <= 4 hours
6	High Availability	Operating System Maturity	Preferred released and QA Tested for >= 6 Months
		Hardware Maturity	Available for purchase for >= 3 Years
		Quality Assurance Certification	Employs a rigorous testing program in a laboratory environment that simulates a “real world” enterprise network. Testing of both hardware and software that verifies feature functionality and interoperability under “real world” traffic loads.

2.3 HIGH-BANDWIDTH CONVERGED I/O ACCESS LAYER SWITCH (10GE HOST CONNECTIVITY)

ID	Primary Attribute	Secondary Attribute	Specification
1	Chassis	Type	Modular
		Rack Mounting	Required
		System Throughput	>= 1 Tbps
		Packet Processor Redundancy Support	Preferred, (See Evaluation Criteria)
		Control Plane Redundancy Support	Preferred, (See Evaluation Criteria)
		Front-Back Airflow Support	Required
		Cooling Redundancy Support	Required
		Power Supply Redundancy Support	Required
		Online Insertion/Removable	Required

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
		Hot-Pluggable	
2	Packet Processor	Type	Integrated
		Layer 3 Switching Throughput (pps)	>= 700 Mpps
		Layer 2 Switching Throughput (pps)	>= 700 Mpps
		Online Insertion/Removal Support	Required when modular
		Memory	>= 1 GB
		L3 Protocols switched in hardware	Preferred: IPv4, IPv6, MPLS, GRE, NAT (See Evaluation Criteria)
3	Linecards/Port Interfaces	Interface Speed	10 Gigabit Ethernet and 1 Gigabit Ethernet
		Media Flexibility Support	Multi-mode fiber, Single-mode fiber, Copper(SFP+, Twin-Axial, UTP)
		Port per ASIC (Oversubscription)	1:1 Preferred
		Throughput to Backplane	n/a
		Queuing Properties	200MB/port w/ Shaped Round Robin + DSCP Support TX: Priority: Preferred, Standard: >= 4 RX: Standard: >= 4
		Online Insertion/Removable Support	Required
		On-Card distributed packet forwarding support	n/a
4	Operating System	Type	Non-Monolithic (Modular) Preferred
		Features Supported	802.1p, 802.1q, Broadcast Storm Control
		Multi-chassis Link Aggregation Support	Required
		Multi-chassis Management	Preferred, (See Implementation Guidance)

ID	Primary Attribute	Secondary Attribute	Specification
		Interface Aggregation	
		Protocols Supported	Required: Jumbo Frames, Link-Layer Discover Protocol, OSPF, BFD / Preferred: CDP, EIGRP
		Network Management	Centralized AAA w/ Role Based Authorization, Syslog SNMP v2c, v3 preferred
5	Support	Technical Support	24x7 Telephone/Web with customer option to immediately escalate to a senior engineer in a network down scenario.
		Parts Replacement	<= 24 hours, preferred <= 4 hours, (See Evaluation Criteria)
6	High Availability	Operating System Maturity	Preferred released and QA Tested for >= 6 Months
		Hardware Maturity	Available for purchase for >= 3 Years
		Quality Assurance Certification	Employs a rigorous testing program in a laboratory environment that simulates a “real world” enterprise network. Testing of both hardware and software that verifies feature functionality and interoperability under “real world” traffic loads.

2.4 VISTA PRIVATE SCS DCI ROUTER/SWITCH - 10MBPS

ID	Primary Attribute	Secondary Attribute	Specification
1	Chassis	Type	Modular
		Rack Mounting	Required
		System Throughput	>= 20,000pps (10Mbps)
		Packet Processor Redundancy Support	Not required
		Control Plane Redundancy Support	Not required
		Front-Back Airflow Support	Required

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
		Cooling Redundancy Support	Required
		Power Supply Redundancy Support	Required
		Online Insertion/Removable Hot-Pluggable	Required
2	Packet Processor	Type	Fixed Configuration
		Layer 3 Switching Throughput (pps)	>= 20,000pps (10Mbps)
		Layer 2 Switching Throughput (pps)	N/A
		Online Insertion/Removal Support	Not required
		Memory	>= 256 MB DRAM, >= 64 MB Flash
		L3 Protocols switched in hardware	Required: IPv4, IPv6, MPLS / Preferred: GRE, NAT
3	Linecards/Port Interfaces	Interface Speed	10/100Mbps Ethernet, DS3 Serial
		Media Flexibility Support	Not required
		Port per ASIC (Oversubscription)	<= 8:1 Preferred
		Throughput to Backplane	>= 1 Gbps
		Queuing Properties	Shaped Round Robin + DSCP Support TX: Priority: Preferred, Standard: >= 4 RX: Standard: >= 4
		Online Insertion/Removable Support	Required
		On-Card distributed packet forwarding support	N/A
4	Operating System	Type	Non-Monolithic (Modular) Preferred

ID	Primary Attribute	Secondary Attribute	Specification
		Features Supported	802.1p, 802.1q, Broadcast Storm Control
		Multi-chassis Link Aggregation Support	Not required
		Multi-chassis Management Interface Aggregation	Not required
		Protocols Supported	Required: Link-Layer Discover Protocol, OSPF, BFD / Preferred: CDP, EIGRP
		Network Management	Centralized AAA w/ Role Based Authorization, Syslog SNMP v2c, v3 preferred
5	Support	Technical Support	24x7 Telephone/Web with customer option to immediately escalate to a senior engineer in a “network down” scenario.
		Parts Replacement	<= 24 hours, preferred <= 4 hours
6	High Availability	Operating System Maturity	Preferred released and QA Tested for >= 6 Months
		Hardware Maturity	Available for purchase for >= 3 Years
		Quality Assurance Certification	Employs a rigorous testing program in a laboratory environment that simulates a “real world” enterprise network. Testing of both hardware and software that verifies feature functionality and interoperability under “real world” traffic loads.

2.5 BLADE SEVER CHASSIS ACCESS LAYER SWITCH (10/100/1000 HOST CONNECTIVITY)

Assumptions: High Availability (Yes/No?) Redundant packet processing? Redundany power supplies?

ID	Primary Attribute	Secondary Attribute	Specification
1	Chassis	Type	Fixed, 2 per Blade Server
		Rack Mounting	N/A
		System Throughput	Up to 128Gbps
		Packet Processor	Not required in single switch. Provided by redundant

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
		Redundancy Support	switches in same blade server
		Control Plane Redundancy Support	Not required
		Front-Back Airflow Support	Not required
		Cooling Redundancy Support	Not required
		Power Supply Redundancy Support	Not required
2	Packet Processor	Type	Modular or non-modular, usually a fixed configuration choice
		Layer 3 Switching Throughput (pps)	35.5Mpps
		Layer 2 Switching Throughput (pps)	35.5Mpps
		Memory	256MB or greater
		Protocols switched in hardware	IPv4, IPv6
3	Interfaces	Interface Speed	1Gb required, 10Gb optional
		ASIC per port	1:1 Preferred
		Throughput to Backplane	N/A
		Queuing Properties	Shaped Round Robin + DSCP Support TX: Priority: Preferred, Standard: >= 4 RX: Standard: >= 4
		Online Insertion/Removable Hot-Pluggable Support	N/A
		On-Card distributed packet forwarding support	N/A
4	Operating System	Type	Modular or Monolithic
		Features Supported	802.1p, 802.1q, Broadcast Storm Control

ID	Primary Attribute	Secondary Attribute	Specification
		Multi-chassis Link Aggregation Support	Required
		Multi-chassis Management Interface Aggregation	Preferred
		Protocols Supported	Required: Jumbo Frames, Link-Layer Discover Protocol, / Preferred: CDP, EIGRP
		Network Management	Centralized AAA w/ Role Based Authorization, Syslog SNMP v2c, v3 preferred
5	Supportability	Technical Support	24x7 Telephone/Web with customer option to immediately escalate to a senior engineer in a “network down” scenario.
		Parts Replacement	<= 24 hours, preferred <= 4 hours
6	High Availability	Operating System Maturity	Preferred released and QA Tested for >= 6 Months
		Hardware Maturity	Available for purchase for >= 3 Years
		Quality Assurance Certification	Employs a rigorous testing program in a laboratory environment that simulates a “real world” enterprise network. Testing of both hardware and software that verifies feature functionality and interoperability under “real world” traffic loads.

2.6 MANAGEMENT ACCESS LAYER SWITCH

ID	Primary Attribute	Secondary Attribute	Specification
1	Chassis	Type	Fixed configuration, Stackable preferred
		Rack Mounting	Required
		System Throughput	24 to 32Gps
		Packet Processor	Not Required

ID	Primary Attribute	Secondary Attribute	Specification
		Redundancy Support	
		Control Plane Redundancy Support	Not Required
		Front-Back Airflow Support	Preferred
		Cooling Redundancy Support	Not Required
		Power Supply Redundancy Support	Preferred, may be supplied with external power supply.
		Online Insertion/Removable Hot-Pluggable	Not Required
2	Packet Processor	Type	Fixed Configuration
		Layer 3 Switching Throughput (pps)	None
		Layer 2 Switching Throughput (pps)	>=13 Mpps
		Online Insertion/Removable Support	Not Required
		Memory	>= 32MB
		Protocols switched in hardware	Layer 2 only, IPv4 and IPv6 packets
3	Linecards/Port Interfaces	Interface Speed	10/100 Megabit Ethernet, 1Gps for uplink interfaces
		Media Flexibility Support	Copper twisted pair with modular type uplink interfaces (copper or fiber). Other interface type may be required in an ad hoc basis.
		Port per ASIC (Oversubscription)	Permitted , <=6:1
		Throughput to Backplane	24 to 32 Gps
		Queuing Properties	TX: >= 4 RX: >= 4
		Online Insertion/Removable	Not Required

ID	Primary Attribute	Secondary Attribute	Specification
		Support	
		On-Card distributed packet forwarding support	Preferred
4	Operating System	Type	Monolithic or Modular
		Features Supported	802.1p, 802.1q, Broadcast Storm Control
		Multi-chassis Link Aggregation Support	Not Required
		Multi-chassis Management Interface Aggregation Support	Not Required , ability to Stack Preferred
		Protocols Supported	Required: LLDP, IPv4 and IPv6 packet support, Preferred: CDP, VTP
		Network Management	Centralized AAA w/ Role Based Authorization, Syslog SNMP v2c, v3 preferred
5	Support	Technical Support	24x7 Telephone/Web with customer option to immediately escalate to a senior engineer in a “network down” scenario.
		Parts Replacement	<= 24 hours, preferred <= 4 hours
6	High Availability	Operating System Maturity	Preferred released and QA Tested for >= 6 Months
		Hardware Maturity	Available for purchase for >= 3 Years
		Quality Assurance Certification	Employs a rigorous testing program in a laboratory environment that simulates a “real world” enterprise network. Testing of both hardware and software that verifies feature functionality and interoperability under “real world” traffic loads.

2.7 LOAD BALANCER

ID	Secondary Attribute	Specification

1	Rack Mountable	Required
2	Load Balancing Predictors	Least loaded, Least Bandwidth, Least Connections, Round-Robin, Hash Address
3	Server Health Monitoring	ICMP, TCP, ECHO(tcp&udp), HTTP, HTTPs, FTP, Telnet, DNS, RADIUS, SNMP, Scripted
4	Redundancy	Required
5	Role-Based Administration	Required
6	Throughput	>= 4 Gbps
7	Packets per Second	>= 6.5 million
8	NAT Entries	>= 1 million
9	Connections per Second	>= 325,000 sustained
10	Concurrent Connections	>= 4 million

3 SUPPORTING DETAILS FOR STANDARDS

3.1 CORE NETWORK SWITCH

It is recognized that the local area network industry is at a juncture in which two competing options could be explored in identifying an appropriate Core switch for the National Data Centers. The increasing popularity of server virtualization, blade server chassis, network attached storage (NAS), and the introduction of the convergence of storage traffic and traditional data traffic onto the LAN has increased the potential need to support higher density 10 gigabit Ethernet.

The current de-facto standard for the current VA Data Centers exploits the Catalyst V-E-Series 6500 as the Core or Aggregation switch. The Catalyst 6500 is a serial cross-bar switch with a total aggregate throughput of 1.44 Terabits per second when configured in a Virtual Switching System (VSS) Model. Cisco has announced plans for a next-generation supervisory module that will double the per-slot throughput to 80 Gigabit increasing the aggregate system throughput to 2.88 Terabits per second in a VSS configuration.

To satisfy high-density 10 gigabit Ethernet requirements at the aggregation and core layers that exceed the capabilities of the Catalyst platform Cisco has introduced the Nexus 7000 which introduces the capability of an aggregate throughput greater than 15 Terabits per second. The Nexus 7000 was announced and started shipping the second quarter of 2008 and is Cisco's next generation Data Center switch and is targeted to replace the Catalyst 6500 in the Data Center.

It has been communicated to the authors of this document that it is the position of the Executive CTO for VA Enterprise Infrastructure Engineering and the Senior Engineering Group that the proliferation of converged I/O and high-densities of 10Gigabit Ethernet in the next three to five years is not imminent. It is therefore the position of this document that the current de-facto standard solution will continue to meet the needs of the organization and therefore should continue to be procured and implemented. When application requirements change necessitating the implementation of a core switch with higher aggregate throughput capacities it will be possible to re-deploy the Catalyst from the core to an access layer.

3.1.1 CHASSIS

STANDARD

ID	***Secondary Attribute***	***Specification***
1	Type	Modular
	Rack Mounting	Required
	System Throughput	>= 1.44 Tbps
	Packet Processor Redundancy Support	Preferred, (See Implementation Guidance)
	Control Plane Redundancy Support	Required
	Front-Back Airflow Support	Required
	Cooling Redundancy Support	Required
	Power Supply Redundancy Support	Required
	Online Insertion/Removable Hot-Pluggable	Required

EXPLANATION OF STANDARD

When there are high density port count requirements that are supporting a mission critical application a modular highly redundant high availability switching architecture will be required. A modular chassis will allow for the upgrade of line-card packet processor modules and interface modules providing the flexibility to replace failed or upgrade obsolete components over time as new technology is introduced.

At the time of the writing of this document, specific data identifying the performance criteria for the applications supported by the Core switching platform was not available; therefore, the authors utilized switching performance data from existing architectures in place today. The system throughput of a switching system, while largely theoretical, does provide a loose scale by which one system can be measured against another. The current throughput requirements of the VA as demonstrated in the currently deployed regional data centers are between one and two Gigabits per second. There is no indication that even with a deployment of 10 Gigabit Ethernet attached virtual servers and storage systems that the VA data center requirements will begin to approach even 100 Gigabits per second of aggregate throughput.

A redundant packet processor is an essential component to a high-availability data network which provides non-stop forwarding and state-full failover during a negative event. Control Plane Redundancy provides the ability to recover from a negative event targeting the router/switch control plane. Additionally a redundant control plane provides the ability to perform in-service software upgrades, take advantage of nonstop forwarding and state-full switchover to a redundant processor.

During normal operation, electrical components of a switching system product heat which is necessary to be dissipated to maintain proper operation. Many implementations of switching systems have a system protection feature that will shut down a system if it overheats. To satisfy a high availability system it is critical to include N+1 redundancy for both cooling and system power.

Front-Back Airflow is a desirable feature to a core network switch that will reside in a data center design and will allow for hot-cold aisle deployment and contribute to more efficient cooling and increased energy efficiency.

Through the lifetime of a system it is occasionally necessary to replace failed components or to upgrade others with more memory or with a next generation component. The ability to replace such component while the system is fully operation with near zero interruption to the normal operation of the system is required in a high availability environment. To facilitate this requirement the chassis must have the capability to support online insertion and removal of “hot-pluggable” components.

EVALUATION FACTORS

- Stability: Will be implemented in a Healthcare environment
- Ability to perform In Service Software Upgrades.
- Slot count of Chassis and Port count of Modules
- Packet Processor Redundancy
- Packet Switching performance
- LAN Protocols and Features supported
- Experience VA currently has with solution

IMPLEMENTATION GUIDANCE

There will be two switches purchased and configured into a Virtual Switching System (VSS) model. If possible each of the switches will be placed in different locations in the data center suite in an effort to mitigate the affect of a negative event within a zone from creating a catastrophic network failure.

Packet processor redundancy is preferred and can be accommodated with a single packet processor in each chassis of a multi-chassis design where the control and data planes are merged between two chassis as is accomplished in the Virtual Switching System (VSS).

As a data center is implemented a concerted effort should be made to ensure that the redundant core switches have physical separation to reduce the impact of an event within a zone of the data center having a global impact on the system. As the data center expands every effort should be made to continue to maintain as much physical separation of the core switches as is reasonably possible.

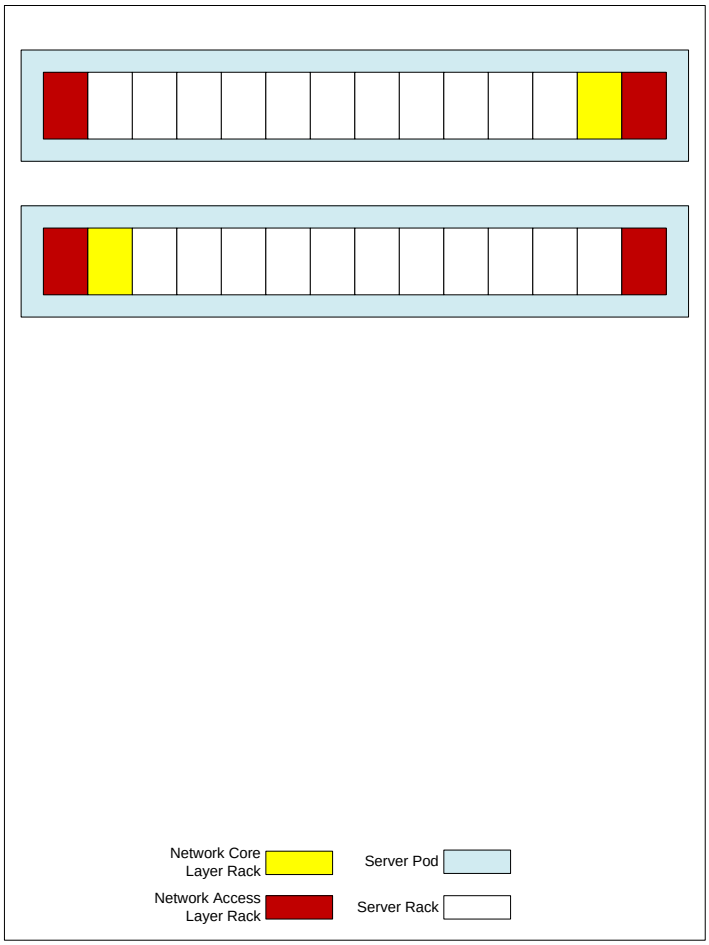


Figure 1 - Initial Implementation of a Data Center

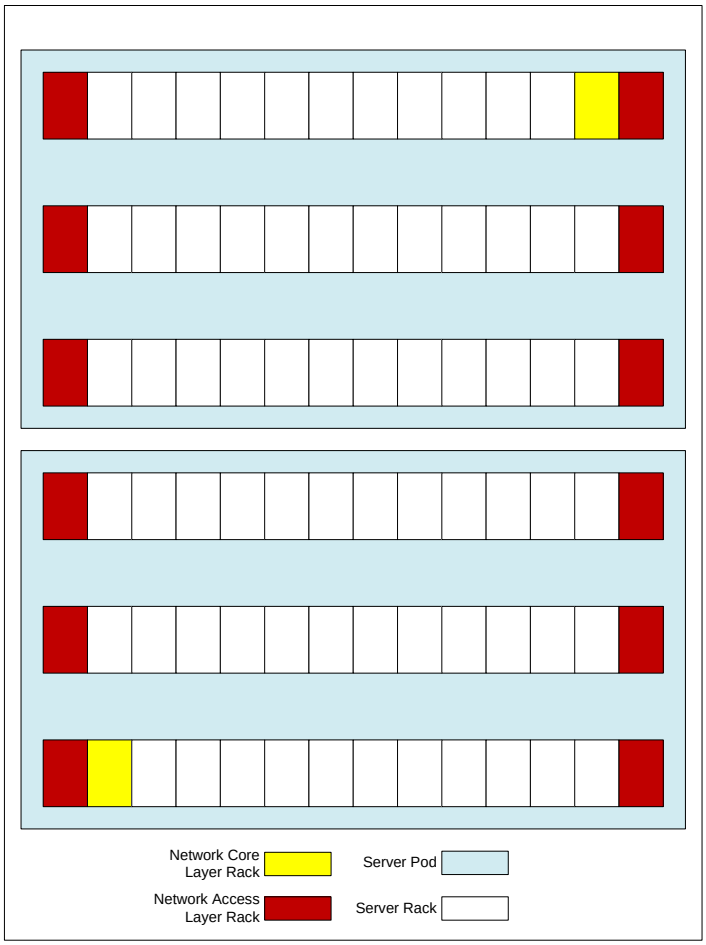


Figure 2 - Expansion of a Data Center

3.1.2 PACKET PROCESSOR

STANDARD

ID	Secondary Attribute	Specification
2	Type	Modular/Upgradable
	Layer 3 Switching Throughput (pps)	>= 450 Mpps
	Layer 2 Switching Throughput (pps)	>= 450 Mpps
	Online Insertion/Removal Support	Required
	Memory	>= 1 GB
	L3 Protocols switched in hardware	Required: IPv4, IPv6, MPLS / Preferred: GRE, NAT

EXPLANATION OF STANDARD

A modular and upgradable packet processor is desirable to allow for the leveraging of new technologies while protecting the investment in purchased interfaces and chassis.

At the time of the writing of this document, specific data identifying the performance criteria for the applications supported by the Core switching platform was not available; therefore, the authors utilized switching performance data from existing architectures in place today. The throughput of a packet processor, while largely theoretical, does provide a loose scale by which one system can be measured against another. The current throughput requirements as demonstrated in the currently deployed regional data centers are between one and two Gigabits per second. There is no indication that even with a deployment of 10 Gigabit Ethernet attached virtual servers and storage systems that the VA data center requirements will begin to approach even 100 Gigabits per second of aggregate throughput.

The capability of a packet processor to allow of online insertion and removal is an essential component to a high-availability network design to allow for in-service technology upgrades and failed component replacement without interrupting critical traffic flows.

The memory of the packet processor translates to the capacity of layer 2 and layer 3 forwarding tables.

The Layer 3 protocols that can be switched in hardware will directly affect the performance of the entire system. A packet processor that can switch critical protocols such as IPv4, IPv6 and MPLS in hardware is a requirement.

EVALUATION FACTORS

- Required support for Multi-Chassis Switch Aggregation feature to support High Availability
- Ability to perform In Service Software Upgrades.
- Stability: Will be implemented in a Healthcare environment
- Packet Switching performance
- LAN Protocols and Features supported
- Experience VA currently has with solution

IMPLEMENTATION GUIDANCE

3.1.3 LINECARDS/PORT INTERFACES

STANDARD

ID	***Secondary Attribute***	***Specification***
3	Interface Speed	10 Gigabit Ethernet and 1 Gigabit Ethernet
	Media Flexibility Support	MMF >= 26m, SMF >= 10km, SMF >= 40km, MMF >= 300m, MMF(850nm)-10GBASE-S, SMF(1310nm)-10GBASE-L, SMF(1550nm)-10GBASE-E, MMF/SMF-10GBASE-LX4, 10GBase-T(Cat6a)
	Port per ASIC (Oversubscription)	1:1 is preferred, See Evaluation Criteria
	Throughput to Backplane	>= 40 Gbps
	Queuing Properties	200MB/port w/ Shaped Round Robin + DSCP Support TX: Priority: Preferred, Standard: >= 4 RX: Standard: >= 4
	Online Insertion/Removable Support	Required
	On-Card distributed	Preferred, See Evaluation Criteria

	packet forwarding support	

EXPLANATION OF STANDARD

Interface Speed- One Gigabit Ethernet Interface speeds will need to be met for Server connectivity. Ten Gigabit Ethernet speeds will need to be supported for Uplinks to Core

Linecards should be able to support a variety of physical media to allow for the flexibility of connecting different technologies over varying distances which can have different tolerances for that are dependent on the media used to transport the signals.

Ports per ASIC (oversubscription) – Depending on performance requirements oversubscription can be perfectly acceptable. As we move to supporting virtualization and I/O convergence resulting in integrating storage technologies onto the LAN the VA will be required to support very minimal oversubscription and therefore the standards will be adapted to leverage solutions and technologies that will support a non-blocking architecture.

The throughput capabilities of a linecard, while largely theoretical, does provide a loose scale by which one component can be measured against another. The standards outlined above demonstrate the current capabilities of deployed systems that are satisfying requirements of the VA now and for the foreseeable future.

Queuing - The queuing properties demonstrate the components ability to allow packets to be en-queued for transmission on a port at a rate greater than the physical medium can support. The ability for port interfaces to have compound buffers and queues translates directly to the performance on the overall system. With compound buffers and queues it becomes possible to classify different applications and assigning appropriate priorities to those traffic flows enabling the system to queue important and time sensitive traffic in front of less important and less time sensitive traffic.

Through the lifetime of a system it is occasionally necessary to replace failed components or to upgrade others with more memory or with a next generation component. The ability to replace such component while the system is fully operation with near zero interruption to the normal operation of the system is required in a high availability environment. To facilitate this requirement the chassis must have the capability to support online insertion and removal of "hot-pluggable" components.

Distributed packet forwarding capabilities of linecards extend the intelligence of forwarding packets between ports on a card, or between similarly capable cards in a chassis directly without requiring the packet to be processed on the system packet processor. This eliminates a “bottle-neck” of traffic flows and allows for a significant performance increase to be realized.

EVALUATION FACTORS

- Ports per ASIC (oversubscription) – The fewer ports that are sharing an ASIC the better the performance. The ideal oversubscription ratio is 1:1.
- On-card distributed packet forwarding support improves performance and is preferred.

IMPLEMENTATION GUIDANCE

If addition hardware is required for full performance it should be required in the original proposal.

3.1.4 OPERATING SYSTEM

STANDARD

ID	*Secondary Attribute*	*Specification*
4	Type	Non-Monolithic (Modular) Preferred
	Features Supported	802.1p, 802.1q, Broadcast Storm Control
	Multi-chassis Link Aggregation Support	Required
	Multi-chassis Management Interface Aggregation	Required
	Protocols Supported	Required: Link-Layer Discover Protocol, OSPF, BFD / Preferred: CDP, EIGRP (See Evaluation Criteria)
	Network Management	Centralized AAA w/ Role Based Authorization, Syslog SNMP v2c, v3 preferred

EXPLANATION OF STANDARD

Type – A modular Operating System is preferred due to its ability to upgrade individual components of the OS. This reinforces the high availability design model.

Features Supported (layer 2) – Specification covers standard layer 2 features supporting high availability and Quality of Service.

Multi-chassis Link Aggregation – Specification is required to support a high availability architecture.

Multi-chassis Management Interface – Managing multiple chassis via a single unified management interface would minimize complexity and would be a preferred method to manage data center switches.

Protocols – Today we rely heavily on CDP to manage data center infrastructure which is Cisco proprietary. LLDP is the standards based Link-Layer Discover Protocol. As a tool to help continue managing the data center the specification requires some form of link layer discovery protocol.

Network Management support – In managing the LAN infrastructure the specified protocols are required to support roles based management, configuration management, and monitoring.

EVALUATION FACTORS

- The CDP protocol is a useful and desirable tool when troubleshooting networks
- The VA uses EIGRP exclusively for VA Medical Centers and EIGRP is highly preferred to leverage existing expertise and maintain compatibility with existing deployments.

IMPLEMENTATION GUIDANCE

3.1.5 SUPPORT

STANDARD

ID	Secondary Attribute	Specification
5	Technical Support	24x7 Telephone/Web with customer option to immediately escalate to a senior engineer in a “network down” scenario.
	Parts Replacement	<= 24 hours, preferred <= 4 hours

EXPLANATION OF STANDARD

The Data Center hardware and software design needs to include the necessary vender support required to maintain the operational state of a Highly Available Data Center.

EVALUATION FACTORS

-

IMPLEMENTATION GUIDANCE

3.1.6 HIGH AVAILABILITY

STANDARD

ID	*Secondary Attribute*	*Specification*
6	Operating System Maturity	Preferred released and QA Tested for >= 6 Months
	Hardware Maturity	Available for purchase for >= 3 Years
	Quality Assurance Certification	Employs a rigorous testing program in a laboratory environment that simulates a "real world" enterprise network. Testing of both hardware and software that verifies feature functionality and interoperability under "real world" traffic loads.

EXPLANATION OF STANDARD

The VA data network supports medical systems that are used in the day-to-day care of patients with applications including the hospital information system, ancillary clinical support systems such as pharmaceutical distribution and bio-diagnostic systems to name a few; all of which are used in the treatment of patients. The availability of the network can influence the information available to providers that are making life-or-death decisions and it therefore becomes critical that the network be available 24x7x365. To support the high availability environment it is essential that the maturity of both the hardware and the supporting software be subjected to a rigorous evaluation of a quality assurance program to mitigate the risk of un-scheduled system down time. The solution should be operating in a non-critical environment for a time sufficient enough to identify any flaws or vulnerabilities that may compromise the stability or security of the system. The more time the system has matured will be directly related to the probability that anomalies will be identified and eliminated and there is a corollary to reduced risk of an outage.

EVALUATION FACTORS

- A minimum of three years available for purchase is desired.

IMPLEMENTATION GUIDANCE

3.2 END-OF-ROW ACCESS LAYER SWITCH (10/100/1000 HOST CONNECTIVITY)

3.2.1 CHASSIS

STANDARD

ID	Secondary Attribute	Specification
1	Type	Modular (Multi-Slot)
	Rack Mounting	Required
	System Throughput	>=720 Mbps
	Packet Processor Redundancy Support	Required
	Control Plane Redundancy Support	Required
	Front-Back Airflow Support	Required
	Cooling Redundancy Support	Required
	Power Supply Redundancy Support	Required
	Online Insertion/Removable Hot-Pluggable	Required

EXPLANATION OF STANDARD

When there are high density port count requirements that are supporting a mission critical application a modular highly redundant high availability switching architecture will be required. A modular chassis will allow for the upgrade of line-card packet processor modules and interface modules providing the flexibility to replace failed or upgrade obsolete components over time as new technology is introduced.

At the time of the writing of this document, specific data identifying the performance criteria for the applications supported by the access switching platform was not available; therefore, the authors utilized switching performance data from existing architectures in place today. The system throughput of a switching system, while largely theoretical, does provide a loose scale by which one system can be measured against another. The current throughput requirements of the VA as demonstrated in the currently deployed regional data centers are between one and two Gigabits per second. There is no indication that even with a deployment of 10 Gigabit Ethernet

attached virtual servers and storage systems that the VA data center requirements will begin to approach even 100 Gigabits per second of aggregate throughput.

A redundant packet processor is an essential component to a high-availability data network which provides non-stop forwarding and state-full failover during a negative event. Control Plane Redundancy provides the ability to recover from a negative event targeting the router/switch control plane. Additionally a redundant control plane provides the ability to perform in-service software upgrades, take advantage of nonstop forwarding and state-full switchover to a redundant processor.

During normal operation, electrical components of a switching system product heat which is necessary to be dissipated to maintain proper operation. Many implementations of switching systems have a system protection feature that will shut down a system if it overheats. To satisfy a high availability system it is critical to include N+1 redundancy for both cooling and system power.

Front-Back Airflow is a desirable feature to a core network switch that will reside in a data center design and will allow for hot-cold aisle deployment and contribute to more efficient cooling and increased energy efficiency.

Through the lifetime of a system it is occasionally necessary to replace failed components or to upgrade others with more memory or with a next generation component. To be able to replace such component while the system is fully operation with near zero interruption to the normal operation of the system is required in a high availability environment. To facilitate this requirement the chassis must have the capability to support online insertion and removal of “hot-pluggable” components.

EVALUATION FACTORS

- Stability: Will be implemented in a Healthcare environment
- Ability to perform In Service Software Upgrades.
- Slot count of Chassis and Port count of Modules
- Packet Processor Redundancy
- Packet Switching performance
- LAN Protocols and Features supported
- Experience VA currently has with solution

IMPLEMENTATION GUIDANCE

3.2.2 PACKET PROCESSOR

STANDARD

ID	Secondary Attribute	Specification
2	Type	Modular/Upgradable
	Layer 3 Switching Throughput (pps)	>= 450 Mpps
	Layer 2 Switching Throughput (pps)	>= 450 Mpps
	Online Insertion/Removable Support	Required
	Memory	>= 1 GB
	Protocols switched in hardware	IPv4, IPv6, MPLS, GRE, NAT (hardware-assisted)

EXPLANATION OF STANDARD

A modular and upgradable packet processor is desirable to allow for the leveraging of new technologies while protecting the investment in purchased interfaces and chassis.

At the time of the writing of this document, specific data identifying the performance criteria for the applications supported by the Core switching platform was not available; therefore, the authors utilized switching performance data from existing architectures in place today. The throughput of a packet processor, while largely theoretical, does provide a loose scale by which one system can be measured against another. The current throughput requirements as demonstrated in the currently deployed regional data centers are between one and two Gigabits per second. There is no indication that even with a deployment of 10 Gigabit Ethernet attached virtual servers and storage systems that the VA data center requirements will begin to approach even 100 Gigabits per second of aggregate throughput.

The capability of a packet processor to allow of online insertion and removal is an essential component to a high-availability network design to allow for in-service technology upgrades and failed component replacement without interrupting critical traffic flows.

The memory of the packet processor translates to the capacity of layer 2 and layer 3 forwarding tables.

The Layer 3 protocols that can be switched in hardware will directly affect the performance of the entire system. A packet processor that can switch critical protocols such as IPv4, IPv6 and MPLS in hardware is a requirement.

EVALUATION FACTORS

- Required support for Multi-Chassis Switch Aggregation feature to support High Availability
- Ability to perform In Service Software Upgrades.
- Stability: Will be implemented in a Healthcare environment
- Packet Switching performance
- LAN Protocols and Features supported
- Experience VA currently has with solution

IMPLEMENTATION GUIDANCE

3.2.3 LINECARDS / PORT INTERFACES

STANDARD

ID	***Secondary Attribute***	***Specification***
3	Interface Speed	10/100 Megabit Ethernet , 1 Gigabit Ethernet & 10 Gigabit Ethernet
	Media Flexibility Support	MMF >= 220m, SMF >= 10km, UTP Cat-5 MMF(850nm)-10GBASE-S, SMF(1310nm)-10GBASE-L, SMF(1550nm)-10GBASE-E, MMF/SMF-10GBASE-LX4
	Port per ASIC (Oversubscription	1:1 Preferred
	Throughput to Backplane	>= 40 Gbps
	Queuing Properties	TX: Priority: Preferred, Standard: >= 4 RX: Standard: >= 4
	Online Insertion/Removable Support	Required
	On-Card distributed packet forwarding support	Preferred

EXPLANATION OF STANDARD

Interface Speed- One Gigabit Ethernet Interface speeds will need to be met for Server connectivity. Ten Gigabit Ethernet speeds will need to be supported for uplinks to Core and to the counter-switch in a VSS configuration

Linecards should be able to support a variety of physical media to allow for the flexibility of connecting different technologies over varying distances which can have different tolerances for that are dependent on the media used to transport the signals.

Ports per ASIC (oversubscription) – Depending on performance requirements oversubscription can be perfectly acceptable. As we move to supporting virtualization and I/O convergence resulting in integrating storage technologies onto the LAN the VA will be required to support very minimal oversubscription and therefore the standards will be adapted to leverage solutions and technologies that will support a non-blocking architecture.

The throughput capabilities of a linecard, while largely theoretical, does provide a loose scale by which one component can be measured against another. The standards outlined above demonstrate the current capabilities of deployed systems that are satisfying requirements of the VA now and for the foreseeable future.

Queuing - The queuing properties demonstrate the components ability to allow packets to be en-queued for transmission on a port at a rate greater than the physical medium can support. The ability for port interfaces to have compound buffers and queues translates directly to the performance on the overall system. With compound buffers and queues it becomes possible to classify different applications and assigning appropriate priorities to those traffic flows enabling the system to queue important and time sensitive traffic in front of less important and less time sensitive traffic.

Through the lifetime of a system it is occasionally necessary to replace failed components or to upgrade others with more memory or with a next generation component. The ability to replace such component while the system is fully operation with near zero interruption to the normal operation of the system is required in a high availability environment. To facilitate this requirement the chassis must have the capability to support online insertion and removal of "hot-pluggable" components.

Distributed packet forwarding capabilities of linecards extend the intelligence of forwarding packets between ports on a card, or between similarly capable cards in a chassis directly without requiring the packet to be processed on the system packet processor. This eliminates a “bottle-neck” of traffic flows and allows for a significant performance increase to be realized.

EVALUATION FACTORS

- Ports per ASIC (oversubscription) – The fewer ports that are sharing an ASIC the better the performance. The ideal oversubscription ratio is 1:1.
- On-card distributed packet forwarding support improves performance and is preferred.

IMPLEMENTATION GUIDANCE

3.2.4 OPERATING SYSTEM

STANDARD

ID	*Secondary Attribute*	*Specification*
4	Type	Non-Monolithic (Modular) Preferred
	Features Supported	802.1p, 802.1q, Broadcast Storm Control
	Multi-chassis Link Aggregation Support	Required
	Multi-chassis Management Interface Aggregation Support	Preferred
	Protocols Supported	Required: Link-Layer Discover Protocol, OSPF, BFD / Preferred: CDP, EIGRP
	Network Management	Centralized AAA w/ Role Based Authorization, Syslog SNMP v2c, v3 preferred, and must be ODBC/JDBC complaint for future integration to the Enterprise Management Framework (EMF).

EXPLANATION OF STANDARD

Type – A modular Operating System is preferred due to its ability to upgrade individual components of the OS. This reinforces the high availability design model

Features Supported (layer 2) – Specification covers standard layer 2 features supporting high availability and Quality of Service.

Multi-chassis Link Aggregation – Specification is required to support a high availability architecture.

Multi-chassis Management Interface – Managing multiple chassis via a single unified management interface would be a preferred method in managing data center switches with simplicity.

Protocols – Today we rely heavily on CDP to manage data center infrastructure which is Cisco proprietary. LLDP is the standards based Link-Layer Discover Protocol. As a tool to help continue managing the data center the specification requires some form of link layer discovery protocol.

Network Management support – In managing the LAN infrastructure the specified protocols are required to support roles based management, configuration management, and monitoring.

EVALUATION FACTORS

- The CDP protocol is a useful and desirable tool when troubleshooting networks

- The VA uses EIGRP exclusively for VA Medical Centers and EIGRP is highly preferred to leverage existing expertise and maintain compatibility with existing deployments.
-

IMPLEMENTATION GUIDANCE

3.2.5 SUPPORT

STANDARD

ID	Secondary Attribute	Specification
5	Technical Support	24x7 Telephone/Web with customer option to immediately escalate to a senior engineer in a “network down” scenario.
	Parts Replacement	<= 24 hours, preferred <= 4 hours

EXPLANATION OF STANDARD

The Data Center hardware and software design needs to include the necessary vender support required to maintain the operational state of a Highly Available Data Center.

EVALUATION FACTORS

-

IMPLEMENTATION GUIDANCE

3.2.6 HIGH AVAILABILITY

STANDARD

ID	Secondary Attribute	Specification
6	Operating System Maturity	Preferred released and QA Tested for >= 6 Months
	Hardware Maturity	Available for purchase for >= 3 Years
	Quality Assurance	Employs a rigorous testing program in a laboratory environment that simulates a

	Certification	"real world" enterprise network. Testing of both hardware and software that verifies feature functionality and interoperability under "real world" traffic loads.

EXPLANATION OF STANDARD

The VA data network supports medical systems that are used in the day-to-day care of patients with applications including the hospital information system, ancillary clinical support systems such as pharmaceutical distribution and bio-diagnostic systems to name a few; all of which are used in the treatment of patients. The availability of the network can influence the information available to providers that are making life-or-death decisions and it therefore becomes critical that the network be available 24x7x365. To support the high availability environment it is essential that the maturity of both the hardware and the supporting software be subjected to a rigorous evaluation of a quality assurance program to mitigate the risk of un-scheduled system down time. The solution should be operating in a non-critical environment for a time sufficient enough to identify any flaws or vulnerabilities that may compromise the stability or security of the system. The more time the system has matured will be directly related to the probability that anomalies will be identified and eliminated and there is a corollary to reduced risk of an outage.

EVALUATION FACTORS

- A minimum of three years available for purchase is desired.
-

IMPLEMENTATION GUIDANCE

3.3 HIGH-BANDWIDTH CONVERGED I/O ACCESS LAYER SWITCH (10GE HOST CONNECTIVITY)

The data center of today is at a juncture in which an evolution of network protocol and physical transport for storage traffic and traditional Ethernet for data are converged onto one media. The increasing popularity of server virtualization, blade server chassis, network attached storage (NAS), and the introduction of the convergence of storage traffic and traditional data traffic onto the LAN has increased the potential need to support higher density 10 gigabit Ethernet.

To satisfy high-density 10 gigabit Ethernet requirements and consolidated I/O such as Fiber Channel over Ethernet (FCoE) in supporting ancillary systems that can be considered "less-than mission critical" it will be advantageous to implement "cutting edge" technology.

3.3.1 CHASSIS

STANDARD

ID	***Secondary Attribute***	***Specification***
1	Type	Static/Modular
	System Throughput	>= 1 Tbps
	Packet Processor Redundancy Support	Preferred, (See Evaluation Criteria)
	Control Plane Redundancy Support	Preferred, (See Evaluation Criteria)
	Front-Back Airflow Support	Preferred, (See Evaluation Criteria)
	Cooling Redundancy Support	Required
	Power Supply Redundancy Support	Required
	Online Insertion/Removable Hot-Pluggable	Required

EXPLANATION OF STANDARD

When there is high-bandwidth or converged I/O (FCoE) requirements a “state-of-the-art” high-capacity switching architecture will be required. A chassis that is static with modular slot for interfaces will allow for the upgrade of line-card interface modules providing the flexibility to replace failed or introduce new components over time.

The system throughput of a switching system, while largely theoretical, does provide a loose scale by which one system can be measured against another. The current throughput requirements of the VA as demonstrated in the currently deployed regional data centers are between one and two Gigabits per second. There is no indication that even with a deployment of 10 Gigabit Ethernet attached virtual servers and storage systems that the VA data center requirements will begin to approach even 100 Gigabits per second of aggregate throughput.

A redundant packet processor is an essential component to a high-availability data network which provides non-stop forwarding and state-full failover during a negative event. Control Plane Redundancy provides the ability to recover from a negative event targeting the router/switch control plane. Additionally a redundant control plane provides the ability to perform in-service software upgrades, take advantage of nonstop forwarding and state-full switchover to a redundant processor.

During normal operation, electrical components of a switching system product heat which is necessary to be dissipated to maintain proper operation. Many implementations of switching systems have a system protection feature that will shut down a system if it overheats. To satisfy a high availability system it is critical to include N+1 redundancy for both cooling and system power.

Front-Back Airflow is a desirable feature to a core network switch that will reside in a data center design and will allow for hot-cold aisle deployment and contribute to more efficient cooling and increased energy efficiency.

Through the lifetime of a system it is occasionally necessary to replace failed components or to upgrade others with more memory or with a next generation component. The ability to replace such component while the system is fully operation with near zero interruption to the normal operation of the system is required in a high availability environment. To facilitate this requirement the chassis must have the capability to support online insertion and removal of “hot-pluggable” components.

EVALUATION FACTORS

- Stability: Will be implemented in a Healthcare environment
- Slot count of Chassis and Port count of Modules
- Packet Switching performance
- LAN Protocols and Features supported
- Experience VA currently has with solution

IMPLEMENTATION GUIDANCE

3.3.2 PACKET PROCESSOR

STANDARD

ID	Secondary Attribute	Specification
2	Type	Preferred Modular/Upgradable, (See Evaluation Criteria)
	Layer 3 Switching Throughput (pps)	>= 700 Mpps
	Layer 2 Switching Throughput (pps)	>= 700 Mpps
	Online Insertion/Removal Support	Required when modular
	Memory	>= 512 MB
	L3 Protocols switched in hardware	n/a

EXPLANATION OF STANDARD

A modular and upgradable packet processor is desirable to allow for the leveraging of new technologies while protecting the investment in purchased interfaces and chassis.

At the time of the writing of this document, specific data identifying the performance criteria for the applications supported by the Core switching platform was not available; therefore, the authors utilized switching performance data from existing architectures in place today. The throughput of a packet processor, while largely theoretical, does provide a loose scale by which one system can be measured against another. The current throughput requirements as demonstrated in the currently deployed regional data centers are between one and two Gigabits per second.

The capability of a packet processor to allow of online insertion and removal is an essential component to a high-availability network design to allow for in-service technology upgrades and failed component replacement without interrupting critical traffic flows.

The memory of the packet processor translates to the capacity of layer 2 and layer 3 forwarding tables.

The Layer 3 protocols that can be switched in hardware will directly affect the performance of the entire system. A packet processor that can switch critical protocols such as IPv4 and IPv6 in hardware is a requirement.

EVALUATION FACTORS

- Stability: Will be implemented in a Healthcare environment
- Packet Switching performance
- Experience VA currently has with solution

IMPLEMENTATION GUIDANCE

3.3.3 LINECARDS/PORT INTERFACES

STANDARD

ID	Secondary Attribute	Specification
3	Interface Speed	10 Gigabit Ethernet and 1 Gigabit Ethernet
	Media Flexibility Support	MMF >= 26m, SMF >= 10km, SMF >= 40km, MMF >= 300m, MMF(850nm)-10GBASE-S, SMF(1310nm)-10GBASE-L, SMF(1550nm)-10GBASE-E, MMF/SMF-10GBASE-LX4, 10GBase-T(Cat6a), TwinAxial(SFP+), 8/4/1 Gbps FiberChannel
	Port per ASIC (Oversubscription)	1:1 Preferred
	Throughput to Backplane	>= 375 Gbps
	Queuing Properties	200MB/port w/ Shaped Round Robin + DSCP Support TX: Priority: Preferred, Standard: >= 4 RX: Standard: >= 4
	Online Insertion/Removable Support	Required
	On-Card distributed packet forwarding support	Preferred

EXPLANATION OF STANDARD

Interface Speed- Ten Gigabit Ethernet Interface speeds with Fiber-Channel over Ethernet (FCoE) capabilities will need to be met for Server connectivity. Ten Gigabit Ethernet speeds will need to be supported for Uplinks to Core

Linecards should be able to support a variety of physical media and both the Ethernet and Fiber-Channel protocols to allow for the flexibility of connecting different technologies over varying distances which can have different tolerances for that are dependent on the media used to transport the signals.

Ports per ASIC (oversubscription) – Depending on performance requirements oversubscription can be perfectly acceptable. As we move to supporting virtualization and I/O convergence resulting in integrating storage technologies onto the LAN the VA will be required to support very minimal oversubscription and therefore the standards will be adapted to leverage solutions and technologies that will support a non-blocking architecture.

Queuing - The queuing properties demonstrate the components ability to allow packets to be en-queued for transmission on a port at a rate greater than the physical medium can support. The ability for port interfaces to

have compound buffers and queues translates directly to the performance on the overall system. With compound buffers and queues it becomes possible to classify different applications and assigning appropriate priorities to those traffic flows enabling the system to queue important and time sensitive traffic in front of less important and less time sensitive traffic.

Through the lifetime of a system it is occasionally necessary to replace failed components or to upgrade others with more memory or with a next generation component. The ability to replace such component while the system is fully operation with near zero interruption to the normal operation of the system is required in a high availability environment. To facilitate this requirement the chassis must have the capability to support online insertion and removal of "hot-pluggable" components.

Distributed packet forwarding capabilities of linecards extend the intelligence of forwarding packets between ports on a card, or between similarly capable cards in a chassis directly without requiring the packet to be processed on the system packet processor. This eliminates a “bottle-neck” of traffic flows and allows for a significant performance increase to be realized.

EVALUATION FACTORS

- Stability: Will be implemented in a Healthcare environment
- Packet Switching performance
- Experience VA currently has with solution

IMPLEMENTATION GUIDANCE

3.3.4 OPERATING SYSTEM

STANDARD

ID	*Secondary Attribute*	*Specification*
4	Type	Non-Monolithic (Modular) Preferred
	Features Supported	802.1p, 802.1q, Broadcast Storm Control
	Multi-chassis Link Aggregation Support	Required
	Multi-chassis Management Interface Aggregation	Preferred
	Protocols Supported	Required: Jumbo Frames, Link-Layer Discover Protocol / Preferred: CDP, EIGRP
	Network Management	Centralized AAA w/ Role Based Authorization, Syslog SNMP v2c, v3 preferred, and must be ODBC/JDBC complaint for future integration to the Enterprise Management Framework (EMF).

EXPLANATION OF STANDARD

Type – A modular Operating System is preferred due to its ability to upgrade individual components of the OS. This reinforces the high availability design model.

Features Supported (layer 2) – Specification covers standard layer 2 features supporting high availability and Quality of Service.

Multi-chassis Link Aggregation – Specification is required to support a high availability architecture.

Multi-chassis Management Interface – Managing multiple chassis via a single unified management interface would minimize complexity and would be a preferred method to manage data center switches.

Protocols – Today we rely heavily on CDP to manage data center infrastructure which is Cisco proprietary. LLDP is the standards based Link-Layer Discover Protocol. As a tool to help continue managing the data center the specification requires some form of link layer discovery protocol.

Network Management support – In managing the LAN infrastructure the specified protocols are required to support roles based management, configuration management, and monitoring.

EVALUATION FACTORS

- Stability: Will be implemented in a Healthcare environment
- Packet Switching performance
- Experience VA currently has with solution

IMPLEMENTATION GUIDANCE

3.3.5 SUPPORT

STANDARD

ID	Secondary Attribute	Specification
5	Technical Support	24x7 Telephone/Web with customer option to immediately escalate to a senior engineer in a “network down” scenario.
	Parts Replacement	<= 24 hours, preferred <= 4 hours

EXPLANATION OF STANDARD

The Data Center hardware and software design needs to include the necessary vender support required to maintain the operational state of a Highly Available Data Center.

EVALUATION FACTORS

-

IMPLEMENTATION GUIDANCE

3.3.6 HIGH AVAILABILITY

STANDARD

ID	Secondary Attribute	Specification
6	Operating System Maturity	Preferred released and QA Tested for >= 6 Months
	Hardware Maturity	Available for purchase for >= 1 Years
	Quality Assurance Certification	Employs a rigorous testing program in a laboratory environment that simulates a "real world" enterprise network. Testing of both hardware and software that verifies feature functionality and interoperability under "real world" traffic loads.

EXPLANATION OF STANDARD

In certain circumstances where there are very high-bandwidth requirements it may be desirable to implement "cutting-edge" technology with the potential for increased performance. Depending on the scenario it may be acceptable to incur a modest amount of risk by implementing a less mature solution as a trade off to a more "state-of-the-art" solution.

EVALUATION FACTORS

•

IMPLEMENTATION GUIDANCE

3.4 VISTA PRIVATE SCS DCI ROUTER/SWITCH - 10MBPS

The private network for VistA supports VMS System Communications Services (SCS). The implementation guidance from HP related to SCS is that there must be 10Mbps of bandwidth available with latency characteristics similar to that of Ethernet. It is imperative that the cluster communications via SCS are maintained to sustain the membership of each node in the cluster. If cluster communication to a node fails then the operation of the entire cluster and processing of the VistA database can be interrupted. Due to the critical nature of this environment it is desirable to have two completely separate and redundant "air-gapped" networks to support the VistA private communications with each database node having a connection to each of the two networks. Since the SCS protocol is extremely resilient and the nodes of the cluster are not prone to adverse effects as a result of an interruption to one of

the private networks as long as the second network is operational, it is acceptable to reduce the design criteria of the network hardware components since high-availability is being achieved in redundancy of the private networks.

3.4.1 CHASSIS

STANDARD

ID	*Secondary Attribute*	*Specification*
1	Type	Modular
	Rack Mounting	Required
	System Throughput	>= 20,000pps (10Mbps)
	Packet Processor Redundancy Support	Not required
	Control Plane Redundancy Support	Not required
	Front-Back Airflow Support	Required
	Cooling Redundancy Support	Required
	Power Supply Redundancy Support	Required
	Online Insertion/Removable Hot-Pluggable	Required

EXPLANATION OF STANDARD

A modular chassis will allow for the upgrade of line-card network interface modules providing the flexibility to replace failed or upgrade obsolete components over time as new technology is introduced.

The requirements for the VistA SCS private network are 10Mbps; therefore, the system throughput should be able to sustain 10Mbps at a minimum.

The high-availability for the VistA SCS private network is achieved in the redundant physical networks; packet processor and control plane redundancy are not required.

During normal operation, electrical components of a switching system produce heat which is necessary to be dissipated to maintain proper operation. Many implementations of switching systems have a system protection

feature that will shut down a system if it overheats. To satisfy a high availability system it is critical to include N+1 redundancy for both cooling and system power.

Front-Back Airflow is a desirable feature to a core network switch that will reside in a data center design and will allow for hot-cold aisle deployment and contribute to more efficient cooling and increased energy efficiency.

Through the lifetime of a system it is occasionally necessary to replace failed components or to upgrade to a next generation component. The ability to replace such component while the system is fully operation with near zero interruption to the normal operation of the system is required in a high availability environment. To facilitate this requirement the chassis must have the capability to support online insertion and removal of "hot-pluggable" components.

EVALUATION FACTORS

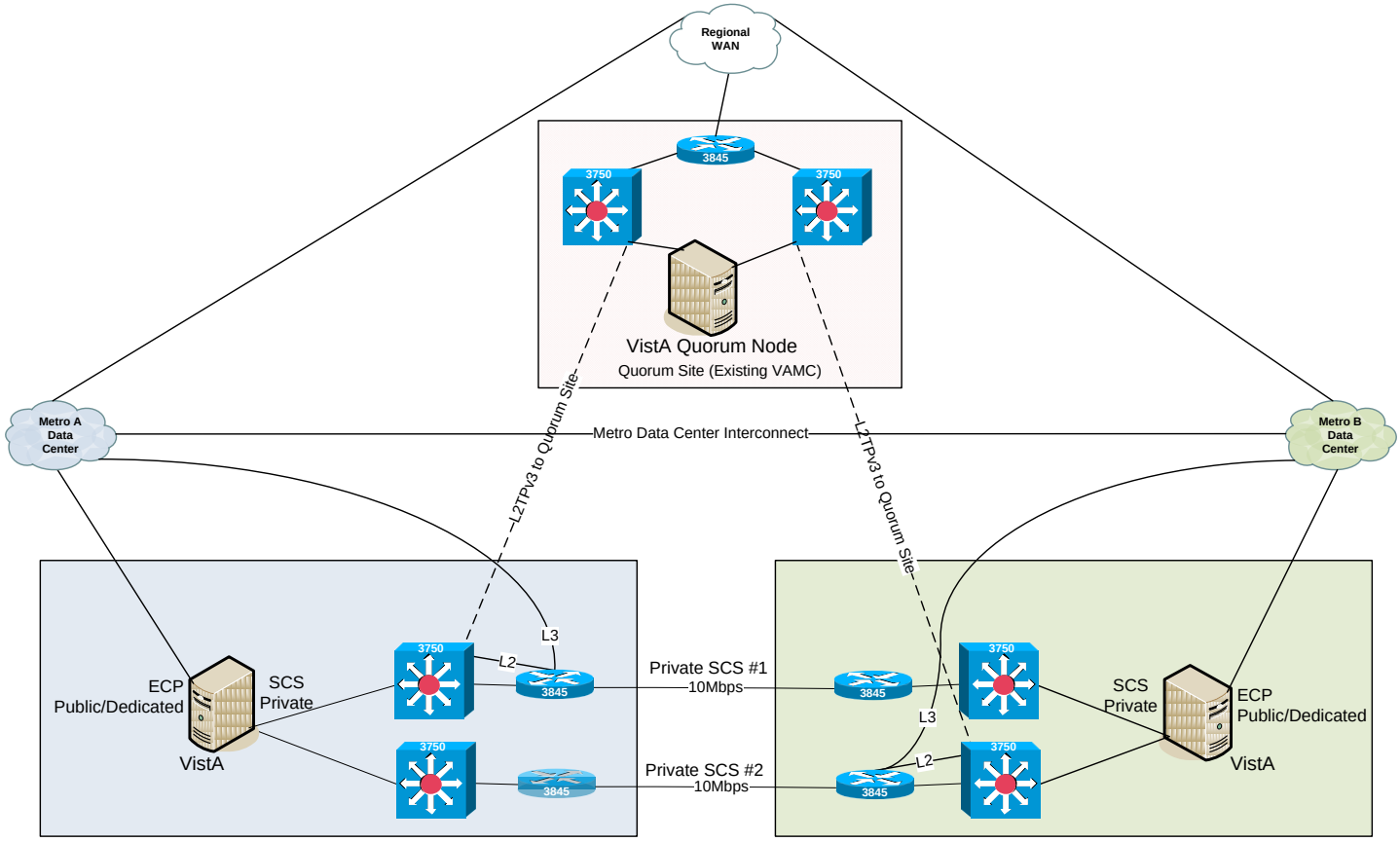
- Stability: Will be implemented in a Healthcare environment
- LAN Protocols and Features supported
- Experience VA currently has with solution

IMPLEMENTATION GUIDANCE

Two independent solutions are required; each vista database node has two private NICs, private NIC #1 and NIC #2 connect to private router/switch #1 and router/switch #2. Two dedicated communication circuits each >= 10Mbps connects Metro data center A and Metro data center B for each SCS private network. A completely separate Spanning-Tree domain is maintained for both Private network SCS #1 and Private network SCS #2.

Each database node will have two private NICs for SCS communications. SCS NIC #1 from each database node will connect to SCS router/switch #1 and SCS NIC #2 from each database node will connect to SCS router/switch #2. The two router/switches SCS #1 and SCS#2 should have sufficient physical separation so as to protect from an event within a zone impacting both switches. To accommodate SCS communication to a quorum site; the SCS router/switch #1 in Metro data center A will be connected to a port that is configured as a L2TPv3 pseudo wire passing the SCS packets through a tunnel routed on the layer 3 network over the regional and/or VA backbone WAN to a port at the quorum site where the SCS NIC #1 from the quorum node is attached. A similar configuration from the SCS switch #2 in Metro data center B, will be connected to a port that is configured as a L2TPv3 pseudo wire passing the SCS packets through a tunnel routed on the layer 3 network to a port at the quorum site where the SCS NIC #2 from the quorum node is attached.

Multi-site SCS Network



3.4.2 PACKET PROCESSOR

STANDARD

ID	Secondary Attribute	Specification
2	Type	Fixed Configuration
	Layer 3 Switching Throughput (pps)	>= 20,000pps (10Mbps)
	Layer 2 Switching Throughput (pps)	N/A

	Online Insertion/Removal Support	Not required
	Memory	>= 256 MB DRAM, >= 64 MB Flash
	L3 Protocols switched in hardware	Required: IPv4, IPv6, MPLS / Preferred: GRE, NAT

EXPLANATION OF STANDARD

The high-availability requirement for the VistA cluster communications is satisfied in the fully redundant physical network; therefore, a lower class router can be employed and a modular and upgradable packet processor is not required in this configuration.

The throughput of a packet processor, while largely theoretical, does provide a loose scale by which one system can be measured against another. The throughput requirements as identified by HP are 10Mbps.

With a static packet processor the capability of a packet processor to allow of online insertion and removal is not required.

The Layer 3 protocols that can be switched in hardware will directly affect the performance of the entire system. A packet processor that can switch critical protocols such as IPv4, IPv6 and MPLS in hardware is a requirement.

EVALUATION FACTORS

- Stability: Will be implemented in a Healthcare environment
- LAN Protocols and Features supported
- Experience VA currently has with solution

IMPLEMENTATION GUIDANCE

3.4.3 LINECARDS/PORT INTERFACES

STANDARD

ID	*Secondary Attribute*	*Specification*
3	Interface Speed	10/100Mbps Ethernet, DS3 Serial
	Media Flexibility Support	Not required
	Port per ASIC (Oversubscription)	<= 8:1 Preferred
	Throughput to Backplane	>= 1 Gbps
	Queuing Properties	Shaped Round Robin + DSCP Support TX: Priority: Preferred, Standard: >= 4 RX: Standard: >= 4
	Online Insertion/Removable Support	Required
	On-Card distributed packet forwarding support	N/A

EXPLANATION OF STANDARD

Interface Speed- Per HP, 10Mbps Ethernet Interface speeds will be sufficient to meet VMS SCS connectivity requirements.

Linecards should be able to support a variety of physical media to allow for the flexibility of connecting different technologies over varying distances which can have different tolerances for that are dependent on the media used to transport the signals.

Ports per ASIC (oversubscription) – The performance requirements of the VMS SCS protocol are very modest and subsequently oversubscription is perfectly acceptable.

Queuing - The queuing properties demonstrate the components ability to allow packets to be en-queued for transmission on a port at a rate greater than the physical medium can support. The ability for port interfaces to have compound buffers and queues translates directly to the performance on the overall system. With compound buffers and queues it becomes possible to classify different applications and assigning appropriate priorities to

those traffic flows enabling the system to queue important and time sensitive traffic in front of less important and less time sensitive traffic.

Through the lifetime of a system it is occasionally necessary to replace failed components or to upgrade others with more memory or with a next generation component. The ability to replace such component while the system is fully operation with near zero interruption to the normal operation of the system is required in a high availability environment. To facilitate this requirement the chassis must have the capability to support online insertion and removal of "hot-pluggable" components.

EVALUATION FACTORS

-

IMPLEMENTATION GUIDANCE

3.4.4 OPERATING SYSTEM

STANDARD

ID	*Secondary Attribute*	*Specification*
4	Type	Non-Monolithic (Modular) Preferred
	Features Supported	802.1p, 802.1q, Broadcast Storm Control
	Multi-chassis Link Aggregation Support	Not required
	Multi-chassis Management Interface Aggregation	Not required
	Protocols Supported	Required: Link-Layer Discover Protocol, OSPF, BFD / Preferred: CDP, EIGRP
	Network Management	Centralized AAA w/ Role Based Authorization, Syslog SNMP v2c, v3 preferred, and must be ODBC/JDBC complaint for future integration to the Enterprise Management Framework (EMF).

EXPLANATION OF STANDARD

Type – A modular Operating System is preferred due to its ability to upgrade individual components of the OS. This reinforces the high availability design model.

Features Supported (layer 2) – Specification covers standard layer 2 features supporting high availability and Quality of Service.

Protocols – Today we rely heavily on CDP to manage data center infrastructure which is Cisco proprietary. LLDP is the standards based Link-Layer Discover Protocol. As a tool to help continue managing the data center the specification requires some form of link layer discovery protocol.

Network Management support – In managing the LAN infrastructure the specified protocols are required to support roles based management, configuration management, and monitoring.

EVALUATION FACTORS

•

3.4.5 SUPPORT

STANDARD

ID	Secondary Attribute	Specification
5	Technical Support	24x7 Telephone/Web with customer option to immediately escalate to a senior engineer in a “network down” scenario.
	Parts Replacement	<= 24 hours, preferred <= 4 hours

EXPLANATION OF STANDARD

The Data Center hardware and software design needs to include the necessary vender support required to maintain the operational state of a Highly Available Data Center.

EVALUATION FACTORS

-

IMPLEMENTATION GUIDANCE

3.4.6 HIGH AVAILABILITY

STANDARD

ID	*Secondary Attribute*	*Specification*
6	Operating System Maturity	Preferred released and QA Tested for >= 6 Months
	Hardware Maturity	Available for purchase for >= 3 Years
	Quality Assurance Certification	Employs a rigorous testing program in a laboratory environment that simulates a "real world" enterprise network. Testing of both hardware and software that verifies feature functionality and interoperability under "real world" traffic loads.

EXPLANATION OF STANDARD

The VA data network supports medical systems that are used in the day-to-day care of patients with applications including the hospital information system, ancillary clinical support systems such as pharmaceutical distribution and bio-diagnostic systems to name a few; all of which are used in the treatment of patients. The availability of the network can influence the information available to providers that are making life-or-death decisions and it therefore becomes critical that the network be available 24x7x365. To support the high availability environment it is essential that the maturity of both the hardware and the supporting software be subjected to a rigorous evaluation of a quality assurance program to mitigate the risk of un-scheduled system down time. The solution should be operating in a non-critical environment for a time sufficient enough to identify any flaws or vulnerabilities that may compromise the stability or security of the system. The more time the system has matured will be directly related to the probability that anomalies will be identified and eliminated and there is a corollary to reduced risk of an outage.

EVALUATION FACTORS

-

IMPLEMENTATION GUIDANCE

3.5 BLADE SEVER CHASSIS ACCESS LAYER SWITCH

3.5.1 CHASSIS

STANDARD

ID	Secondary Attribute	Specification
1	Type	Fixed, 2 per Blade Server
	Slot Count	N/A, fixed configuration (usually)
	Maximum Theoretical System Throughput	Up to 128Gbps
	Packet Processor Redundancy Support	Not required in single switch. Provided by redundant switches in same blade server
	Control Plane Redundancy Support	Not required
	Front-Back Airflow Support	Not required
	Cooling Redundancy Support	Not required
	Power Supply Redundancy Support	Not required

EXPLANATION OF STANDARD

Certain server platforms deployed by the VA will consist of Blade Server Chassis'. All Blade Servers typically contain two internal network switches to provide connectivity for the internal server blades. This standard defines the properties required for these switches. Most Blade Server manufacturers will provide a limited choice in switch type included with each server model. These choices are usually fixed configurations but may vary between server manufacturer.

Since the Blade Server switch implementations are usually offered as fixed configurations with very small form factors, many of the standard chassis requirements are either not applicable or can't be met by any manufacturer. Air flow and cooling are typically provided by the Blade Server fans themselves and not in the switches.

All Blade Server manufacturers should offer redundant internal switches as a standard option. This is a requirement. Typical Blade Server implementations utilize direct switch backplane connections to the individual blade servers and then multiple external 1Gig or 10Gig interfaces for uplinks to external switch environments.

EVALUATION FACTORS

- Stability: Will be implemented in a Healthcare environment
- Experience VA currently has with solution

IMPLEMENTATION GUIDANCE

3.5.2 PACKET PROCESSOR

STANDARD

ID	*Secondary Attribute*	*Specification*
1	Type	Modular or non-modular, usually a fixed configuration choice
	Layer 3 Switching Throughput (pps)	35.5Mpps
	Layer 2 Switching Throughput (pps)	35.5Mpps
	Multi-chassis Link Aggregation Support	Required
	Memory	256MB or greater
	Protocols switched in hardware	IPv4, IPv6 preferred

EXPLANATION OF STANDARD

Multi-chassis Link Aggregation support is the most important feature in this section. The VA has set a requirement that Multi-chassis Link Aggregation will be used to connect all non-Vista servers within the datacenters. What this means for the Blade Server switches is that both internal server switches must be able to bond all uplink ports to a single aggregated port channel and then bond all backplane connections to a one server to a single aggregated port channel. Each server will need it's own aggregated port channel.

At the time of the writing of this document, specific data identifying the performance criteria for the applications supported by the Core switching platform was not available; therefore, the authors utilized switching performance data from existing architectures in place today. The throughput of a packet processor, while largely theoretical, does provide a loose scale by which one system can be measured against another. The current throughput requirements as demonstrated in the currently deployed regional data centers are between one and two Gigabits per second. There is no indication that even with a deployment of 10 Gigabit Ethernet attached virtual servers and storage systems that the VA data center requirements will begin to approach even 100 Gigabits per second of aggregate throughput.

The Layer 3 protocols that can be switched in hardware will directly affect the performance of the entire system. A packet processor that can switch critical protocols such as IPv4 and IPv6 in hardware is a preference.

EVALUATION FACTORS

- Stability: Will be implemented in a Healthcare environment

- Packet Switching performance
- Experience VA currently has with solution

IMPLEMENTATION GUIDANCE

3.5.3 INTERFACES

STANDARD

ID	Secondary Attribute	Specification
1	Interface Speed	1Gb required, 10Gb optional
	Interface Count	4-8+ 1Gbps or 2+ 10Gbps
	ASIC per port	1:1 Preferred
	Throughput to Backplane	N/A
	Queuing Properties	Shaped Round Robin + DSCP Support TX: Priority: Preferred, Standard: >= 4 RX: Standard: >= 4

EXPLANATION OF STANDARD

Typical Blade Server switches utilize backplane connections for the direct internal blade server uplink ports. External ports are provided to uplink the Blade Server switches to existing external switch fabrics.

Ports per ASIC (oversubscription) – Depending on performance requirements oversubscription can be perfectly acceptable. As we move to supporting virtualization and I/O convergence resulting in integrating storage technologies onto the LAN the VA will be required to support very minimal oversubscription and therefore the standards will be adapted to leverage solutions and technologies that will support a non-blocking architecture.

Queuing - The queuing properties demonstrate the components ability to allow packets to be en-queued for transmission on a port at a rate greater than the physical medium can support. The ability for port interfaces to have compound buffers and queues translates directly to the performance on the overall system. With compound buffers and queues it becomes possible to classify different applications and assigning appropriate priorities to those traffic flows enabling the system to queue important and time sensitive traffic in front of less important and less time sensitive traffic.

Certain specific switch port protocol features are required in order provide continuity with existing configurations. The above list is based on current VA implementations and existing server software capabilityes (Virtual Environments).

EVALUATION FACTORS

- Stability: Will be implemented in a Healthcare environment

- Packet Switching performance
- Experience VA currently has with solution
- Interface counts: 4-8+ 1Gbps or 2+ 10Gbps
- Desirable Protocols include LACP and IGMP snooping

IMPLEMENTATION GUIDANCE

3.5.4 OPERATING SYSTEM

STANDARD

ID	Secondary Attribute	Specification
1	Type	Monolithic or Modular
	Features Supported	802.1p, 802.1q, Broadcast Storm Control
	Multi-chassis Link Aggregation	Required
	Multi-chassis Management Interface Aggregation	Preferred
	Protocols Supported	Required: Jumbo Frames, Link-Layer Discover Protocol, / Preferred: CDP, EIGRP
	Network Management	Centralized AAA w/ Role Based Authorization, Syslog SNMP v2c, v3 preferred, and must be ODBC/JDBC complaint for future integration to the Enterprise Management Framework (EMF).

EXPLANATION OF STANDARD

Since typical Blade Server switch implementations are fixed configurations, the operating system type (modular vs. non-modular) isn't as critical as with other environments.

Features Supported (layer 2) – Specification covers standard layer 2 features supporting high availability and Quality of Service.

Protocols – Today we rely heavily on CDP to manage data center infrastructure which is Cisco proprietary. CDP is also provided as an option with VMWare operating systems and becomes very useful when interacting with ESX server environments. LLDP is the standards based Link-Layer Discover Protocol. As a tool to help continue managing the data center the specification requires some form of link layer discovery protocol.

EVALUATION FACTORS

- Stability: Will be implemented in a Healthcare environment
- LAN Protocols and Features supported
- Experience VA currently has with solution

3.5.5 SUPPORT

STANDARD

ID	Secondary Attribute	Specification
5	Technical Support	24x7 Telephone/Web with customer option to immediately escalate to a senior engineer in a “network down” scenario.
	Parts Replacement	<= 24 hours, preferred <= 4 hours

EXPLANATION OF STANDARD

The Data Center hardware and software design needs to include the necessary vender support required to maintain the operational state of a Highly Available Data Center.

EVALUATION FACTORS

-

IMPLEMENTATION GUIDANCE

3.5.6 HIGH AVAILABILITY

STANDARD

ID	Secondary Attribute	Specification
6	Operating System Maturity	Preferred released and QA Tested for >= 6 Months
	Hardware Maturity	Available for purchase for >= 3 Years
	Quality Assurance Certification	Employs a rigorous testing program in a laboratory environment that simulates a "real world" enterprise network. Testing of both hardware and software that verifies feature functionality and interoperability under "real world" traffic loads.

EXPLANATION OF STANDARD

The VA data network supports medical systems that are used in the day-to-day care of patients with applications including the hospital information system, ancillary clinical support systems such as pharmaceutical distribution and bio-diagnostic systems to name a few; all of which are used in the treatment of patients. The availability of the network can influence the information available to providers that are making life-or-death decisions and it therefore becomes critical that the network be available 24x7x365. To support the high availability environment it is essential that the maturity of both the hardware and the supporting software be subjected to a rigorous evaluation of a quality assurance program to mitigate the risk of un-scheduled system down time. The solution should be operating in a non-critical environment for a time sufficient enough to identify any flaws or vulnerabilities that may compromise the stability or security of the system. The more time the system has matured will be directly related to the probability that anomalies will be identified and eliminated and there is a corollary to reduced risk of an outage.

EVALUATION FACTORS

-

IMPLEMENTATION GUIDANCE

3.6 MANAGEMENT ACCESS LAYER SWITCH

Most servers come with a remote management interfaces (RMIs). These management interfaces vary in designation by manufacturer IGO, RILO, and RMOC are examples). They permit remote access to perform basic management functions and allow connectivity when the server is in an impaired state. As a normal business process managers access the servers via RDP. RMIs are therefore a redundant or alternate connection path.

RMIs have low to medium density port count and limited traffic requirements. Due to the limited density and traffic requirements and alternate access methods a fixed configuration, non-redundant switching architecture will be required. Stackable switches with redundant power supply options are preferred.

3.6.1 CHASSIS

STANDARD

ID	***Secondary Attribute***	***Specification***
1	Type	Fixed configuration, Stackable preferred
	Rack Mounting	Required
	System Throughput	24 to 32Gps
	Packet Processor Redundancy Support	Not Required
	Control Plane Redundancy Support	Not Required
	Front-Back Airflow Support	Preferred
	Cooling Redundancy Support	Not Required
	Power Supply Redundancy Support	Preferred, may be supplied with external power supply.
	Online Insertion/Removable Hot-Pluggable	Not Required

EXPLANATION OF STANDARD

Front-Back Airflow is a desirable feature due to the hot-cold aisle VA data center design standard.

Due to RMI access being just one of many ways to access servers a minimal amount of RMI access downtime is acceptable.

EVALUATION FACTORS

- None

IMPLEMENTATION GUIDANCE

- None

3.6.2 PACKET PROCESSOR

STANDARD

ID	*Secondary Attribute*	*Specification*
2	Type	Fixed Configuration
	Layer 3 Switching Throughput (pps)	None
	Layer 2 Switching Throughput (pps)	>=13 Mpps
	Online Insertion/Removable Support	Not Required
	Memory	>= 32MB
	Protocols switched in hardware	Layer 2 only, IPv4 and IPv6 packets

EXPLANATION OF STANDARD

A fixed configuration packet processor is desirable due to the low bandwidth requirements and the availability of alternate connectivity.

All layer three (routing) functions will reside with higher level devices.

Online insertion and removal is not required as this is an alternate method of connectivity and short periods of downtime for this device is permitted.

EVALUATION FACTORS

- None

IMPLEMENTATION GUIDANCE

- None

3.6.3 PORT INTERFACES

STANDARD

ID	*Secondary Attribute*	*Specification*
3	Interface Speed	10/100 Megabit Ethernet, 1Gps for uplink interfaces
	Media Flexibility Support	Copper twisted pair with modular type uplink interfaces (copper or fiber). Other interface type may be required in an ad hoc basis.
	Port per ASIC (Oversubscription)	Permitted , <=6:1
	Throughput to Backplane	24 to 32 Gps
	Queuing Properties	TX: >= 4 RX: >= 4
	Online Insertion/Removable Support	Not Required

EXPLANATION OF STANDARD

Interface Speed - Management access layer switches and RMIs have limited traffic requirements therefore only 10/100Mbs is required.

Medical Flexibility Support - Remote Management Interfaces are usually of the UTP type.

Ports per ASIC (oversubscription) - Due to low performance requirements oversubscription can is acceptable.

Throughput to Backplane - The throughput capabilities of a backplane, while largely theoretical, does provide a loose scale by which one component can be measured against another. The standards outlined above demonstrate the current capabilities of deployed systems that are satisfying requirements of the VA now and for the foreseeable future.

Queuing - The queuing properties demonstrate the components ability to allow packets to be en-queued for transmission on a port at a rate greater than the physical medium can support. The ability for port interfaces to have compound buffers and queues translates directly to the performance on the overall system. With compound buffers and queues it becomes possible to classify different applications and assigning appropriate priorities to those traffic flows enabling the system to queue important and time sensitive traffic in front of less important and less time sensitive traffic.

Online Insertion/Removable Support - Online insertion and removal is not required as this is an alternate method of connectivity and short periods of downtime for this device is permitted.

EVALUATION FACTORS

- None

IMPLEMENTATION GUIDANCE

- None

3.6.4 OPERATING SYSTEM

STANDARD

ID	***Secondary Attribute***	***Specification***
4	Type	Monolithic or Modular
	Features Supported	802.1p, 802.1q, Broadcast Storm Control
	Multi-chassis Link Aggregation Support	Not Required
	Multi-chassis Management Interface Aggregation Support	Not Required , ability to Stack Preferred

	Protocols Supported	Required: LLDP, IPv4 and IPv6 packet support, Preferred: CDP, VTP
	Network Management	Centralized AAA w/ Role Based Authorization, Syslog SNMP v2c, v3 preferred, and must be ODBC/JDBC complaint for future integration to the Enterprise Management Framework (EMF).

EXPLANATION OF STANDARD

Type – A modular Operating System is usually not associated with the type of switch but is acceptable.

Features Supported (layer 2) – Specification covers standard layer 2 features supporting Quality of Service.

Multi-chassis Link Aggregation – Not required

Multi-chassis Management Interface – Managing multiple chassis via a single unified management interface would be a preferred method in managing data center switches with simplicity.

Protocols – Today we rely heavily on CDP to manage data center infrastructure which is Cisco proprietary. LLDP is the standards based Link-Layer Discover Protocol. As a tool to help continue managing the data center the specification requires some form of link layer discovery protocol.

Network Management support – In managing the LAN infrastructure the specified protocols are required to support roles based management, configuration management, and monitoring.

EVALUATION FACTORS

- None

IMPLEMENTATION GUIDANCE

- None

3.6.5 SUPPORT

STANDARD

ID	***Secondary Attribute***	***Specification***
5	Technical Support	24x7 Telephone/Web with customer option to immediately escalate to a senior engineer in a “network down” scenario.
	Parts Replacement	<= 24 hours, preferred <= 4 hours

EXPLANATION OF STANDARD

The Data Center hardware and software design needs to include the necessary vender support required to maintain the operational state of a Highly Available Data Center.

EVALUATION FACTORS

- None

IMPLEMENTATION GUIDANCE

- None

3.6.6 HIGH AVAILABILITY

STANDARD

ID	***Secondary Attribute***	***Specification***
6	Operating System Maturity	Preferred released and QA Tested for >= 6 Months
	Hardware Maturity	Available for purchase for >= 1 Year
	Quality Assurance Certification	Employs a rigorous testing program in a laboratory environment that simulates a "real world" enterprise network. Testing of both hardware and software that verifies feature functionality and interoperability under "real world" traffic loads.

EXPLANATION OF STANDARD

To support the high availability environment it is essential that the maturity of both the hardware and the supporting software be subjected to a rigorous evaluation of a quality assurance program to mitigate the risk of un-scheduled system down time. The solution should be operating in a non-critical environment for a time sufficient enough to identify any flaws or vulnerabilities that may compromise the stability or security of the system. The more time the system has matured will be directly related to the probability that anomalies will be identified and eliminated and there is a corollary to reduced risk of an outage.

EVALUATION FACTORS

- None

IMPLEMENTATION GUIDANCE

- None

3.7 LOAD BALANCER

STANDARD

ID	Secondary Attribute	Specification
1	Rack Mountable	Required
2	Load Balancing Predictors	Least loaded, Least Bandwidth, Least Connections, Round-Robin, Hash Address
3	Server Health Monitoring	ICMP, TCP, ECHO(tcp&udp), HTTP, HTTPs, FTP, Telnet, DNS, RADIUS, SNMP, Scripted
4	Redundancy	Required
5	Role-Based Administration	Required
6	Throughput	>= 4 Gbps
7	Packets per Second	>= 6.5 million
8	NAT Entries	>= 1 million
9	Connections per Second	>= 325,000 sustained
10	Concurrent Connections	>= 4 million

EXPLANATION OF STANDARD

EVALUATION FACTORS

•

IMPLEMENTATION GUIDANCE

The solution will employ a system that will probe each of the database nodes in both metro data centers to determine which of the metro pairs the target database in currently operating in. The solution will then probe a pool of applications nodes to determine which of the pool within the data center hosting the database are receiving connections for the target data base. The solution will then measure the current loading on each of the

eligible application nodes to determine the least loaded node. The solution will then send connections to the least loaded node.

4 TAXONOMY OF STANDARDS

The primary and secondary attributes identified below are common to all standards sets that will be contained in this standard.

ID	*Primary Attribute*	*Secondary Attribute*
1	Chassis	Type (Modular vs. Static)
		Rack Mounting
		System Throughput
		Packet Processor Redundancy Support
		Control Plane Redundancy Support
		Cooling Redundancy Support
		Power Supply Redundancy Support
		Front-Back Airflow Support
		Online Insertion/Removable Hot-Pluggable Support
2	Packet Processor	Type (Upgradable)
		Layer 3 Switching Throughput (pps)
		Layer 2 Switching Throughput (pps)
		Online Insertion/Removable Hot-Pluggable Support
		Memory
		Protocols switched in hardware
3	Linecards	Interface Speed
		Interface Media Flexibility Support
		ASIC per port (Oversubscription)
		Throughput to Backplane

		Queuing Properties
		Online Insertion/Removable Hot-Pluggable Support
		On-Card distributed packet forwarding support
4	Operating System	Type (Modular)
		Features Supported
		Multi-chassis Link Aggregation
		Multi-chassis Management Interface Aggregation
		Protocols Supported
		Network Management
5	Supportability	Technical Support
		Parts replacement
6	High Availability	Operating System Maturity
		Hardware Maturity
		Quality Assurance Certification
7	Load Balancer	Rack Mountable
		Load Balancing Predictors
		Server Health Monitoring
		Connection Persistence
		Redundancy
		Role-Based Administration
		Throughput
		Packets per Second
		Probes
		NAT Entries
		Connections per Second

		Concurrent Connections
8	Metropolitan Data Center Interconnect (MAN)	Latency
		Transport Method
		Reliability/SLA/Packet Loss
		Path Diversity (Includes Local Loop)
		Carrier Diversity
		Capacity
		Quality of Service
		Networx Carriers
		Traffic Analysis / Probes

APPENDIX A – DEFINITIONS

Click here to enter definitions.

APPENDIX B – REFERENCES

Click here to enter a list of references.

APPENDIX C – ACRONYMS

Refer to the VA Acronym Lookup Web page for a list of VA specific acronyms.

EIE VA OI&T Enterprise Infrastructure Engineering

MEC Multi-Chassis Etherchannel

vPC Virtual Port Channel

VSS Virtual Switching System

FCoE Fiber Channel over Ethernet

APPENDIX D – CONTRIBUTORS

The following subject matter experts have contributed to the development of this document as indicated

Name	Organization	Role
Marty Trey	Enterprise Infrastructure Engineering	Team Lead
Tim Dahl	Enterprise Infrastructure Engineering	SME
Gary Benson	Field Operations & Development, Region 1	SME
Mike Cunagin	Contractor representing Region 1	SME
Allen Stevens	Field Operations & Development, Region 1	SME
Hal Haislip	Field Operations & Development, Region 2	SME
Rich Colby	Field Operations & Development, Region 3	SME
Juan Adames	Field Operations & Development, Region 3	SME
Gary Branch	Field Operations & Development, Region 4	SME
Anthony Paul	Field Operations & Development, Region 5	SME
David Polanco	Field Operations & Development, VACO	SME
Casey O'Brien	Field Operations & Development, CDCO	SME
John Mehl	Field Operations & Development, PMO	Stake Holder Representative

John Hina	Field Implementation Services	Stake Holder Representative
Robert Moser	Field Implementation Services	Stake Holder Representative

DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INFORMATION AND TECHNOLOGY

ENTERPRISE INFRASTRUCTURE ENGINEERING

VA Enterprise IT Infrastructure Standard

Wide Area Network

Production 1.0

November 30, 2009

TABLE OF CONTENTS

1 Introduction 1

1.1 Purpose 1

1.2 Objectives 1

1.3 Scope 1

2 Standards 2

2.1 Class A Router 2

2.2 Class B Router 4

2.3 Wide Area Network 6

2.3.1 Metro Data Center To Backbone 6

2.3.2 Metro Data Center To Region WAn 6

2.3.3 Medical Center To Region WAN 7

2.3.4 Medical Center Branch Office To Region WAN 8

2.4 WAN Encryption 9

2.4.1 Data Center 9

2.4.2 Medical Center 9

2.5 WAN Acceleration 10

2.5.1 Data Center 10

2.5.2 Medical Center 11

3 Supporting Details for Standards 12

3.1 CLass A Router – OC3(qty:4) and higher 12

3.1.1 CHASSIS 12

3.1.2 Packet Processor 13

3.1.3 Interface Cards 15

3.1.4 Operating System 16

3.1.5 WAN Encryption 18
3.1.6 Platform Supportability 20
3.1.7 Platform Maturity 21
3.2 Class B Router – DS3(qty:4) up to OC3(qty:3) 22
3.2.1 Chassis 22
3.2.2 Packet Processor 24
3.2.3 Interface Cards 25
3.2.4 Operating System 26
3.2.5 WAN Encryption 28
3.2.6 platform supportability 30
3.2.7 Platform maturity 31
3.3 Wide Area Network 31
3.3.1 Metro Data Center To Backbone 31
3.3.2 Metro Data Center to Region WAN 34
3.3.3 Medical Center to Region WAN 35
3.3.4 Medical Center Branch Office to Region WAN 39
3.4 WAN Encryption 40
3.4.1 Data Center 40
3.4.2 Medical Center 42
3.5 WAN Acceleration 44
3.5.1 Data Center 44
3.5.2 Medical Center 47
4 Taxonomy of Standards 50
Appendix A – Definitions 53
Appendix B – References 53
Appendix C – Acronyms 53
Appendix D – Contributors 53

Appendix E – MPLS SLA..... 53

1 INTRODUCTION

1.1 PURPOSE

A standard is a set of rules or requirements that are determined by a consensus opinion of subject matter experts and prescribe criteria for a product, process, test or procedure. The general benefits of a standard are quality, interchangeability of parts or systems, and consistency. Information Technology (IT) standards are based on business needs provided through or supported by IT Services. IT Services are designed to support business processes and are constructed from software, hardware and infrastructure components. Establishing and enforcing standards for the selection and configuration of these supporting components improves the maintainability, reliability and availability of IT Services within projected economic constraints in alignment with business needs.

This standards document lists the acceptable and recommended specifications for Wide Area Network. Sections include standard specifications for subject components, decisions supporting the standard specifications, guidelines or recommendations for implementing the standard specifications, and supplemental factors to consider when evaluating subject components. Other supplementary documents will provide guidance on procuring components that meet the standard specifications, guidance on integrating them with existing components, and explanation of how the subject components fit into the VA Architecture.

1.2 OBJECTIVES

This standard provides acceptable and recommended specifications to support:

- Solution Evaluation
- Requirement Evaluation
- Solution Design
- Solution Procurement and Bid Evaluation
- Evaluation of Architectural Specifications
- Provide vendor neutral, or vendor specific where justified, specifications needed to support the design of the VA WAN Infrastructure.

1.3 SCOPE

This standard applies to:

- WAN Infrastructure providing connectivity to the National Data Centers

2 STANDARDS

2.1 CLASS A ROUTER

Class "A" or Carrier class router transporting high volumes of traffic where service disruption is unacceptable.

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
1	Chassis	Type (Modular vs. Static)	Required: Modular
		Throughput	Backplane performance of >= 15 Millions packets per second
		Packet Processor Redundancy	Required
		Control Plane Redundancy	Required
		Cooling Redundancy	Required: May be internal to power supplies
		Power Supply Redundancy	Required
		Front-Back Airflow	Required
		Online Insertion & Removal	Required
2	Packet Processor	Type (upgradable)	Required (not integral to chassis)
		Packet Processor Redundancy	Required
		Layer 3 Routing Throughput (PPS)	>= 15 Million packets per second
		Online Insertion & Removal	Required
		Memory (DRAM, Flash)	Upgradeable - Volatile >= 2GB, Non-Volatile >= 1GB
3	Interface Cards	Interface Speed	Up to 10Gbps
		Interface Media Flexibility	Required (from T-1 to 10Gbps interfaces) T-1, channelized T-1, DS-3, channelized DS-3, OC-3 to OC12, OC-3 to OC-12 Packet over SONET, 10Mbps to 10Gbps Ethernet, at a minimum. (see Evaluation Factors)

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
		Queuing Properties	Required: see 3.1.3 Operating System
		Online Insertion & Removal	Required
4	Operating System	Type (Modular)	Preferred (See Implementation Guidance)
		Features Supported	Required: Routing, Bridging, Switching
		Routing Protocols	Required: BGPv4, OSPF, Preferred: EIGRP (See Evaluation Criteria)
		Quality of Service	Required: including shaping and policing
		Protocols Supported	Required: MPLS, IPv4, IPv6, 802.1Q, GRE, IPSEC, GDOI
		Network Management	Required: SNMPv1 thru 3, SSH, SSL, IP-SLA, Syslog, Traps (See evaluation criteria for IP Flow export)
5	WAN Encryption	FIPS 140-2 Certification	Required: Complete, or in process. (See Implementation Guidance)
		Throughput	Required: >= 5Gbps (Inbound/Outbound Aggregate) (See Evaluation Criteria)
		Hardware vs Software	Required: Hardware
		Latency	Required: <=100usec
		Performed using Encapsulation(Tunneling) vs. Payload	Payload preferred, (See Implementation Guidance)
		Supported Connection Count	Required: >=2000 encrypted tunnels
		Interface Type	Required: Encryption Supported on all interface types
6	Platform Supportability	Technical Support	Required: Phone support 7x24x365
		Parts Replacement	Required: With onsite 4 hour replacement
7	Platform Maturity	Operating System Maturity	Required, 1 year in general production

ID	Primary Attribute	Secondary Attribute	Specification
		Hardware Maturity	Required, 1 year in general production
		Quality Assurance Certification	Employs a rigorous testing program in a laboratory environment that simulates a "real world" enterprise network. Testing of both hardware and software that verifies feature functionality and interoperability under "real world" traffic loads.

2.2 CLASS B ROUTER

Class "B" Router transports high volumes of traffic, needs redundancy, but does not require higher speed interface density.

ID	Primary Attribute	Secondary Attribute	Specification
1	Chassis	Type (Modular vs. Static)	Modular required
		System Throughput	2 Million pps
		Packet Processor Redundancy	Preferred
		Control Plane Redundancy	Preferred
		Cooling Redundancy	Preferred
		Power Supply Redundancy	Required
		Front-Back Airflow	Preferred
		Online Insertion & Removal	Required
2	Packet Processor	Type (upgradable)	Required
		Packet Processor Redundancy	Preferred
		Layer 3 Routing Throughput (pps)	2 Million pps
		Online Insertion & Removal	Preferred
		Memory (DRAM, Flash)	1 GB – DRAM, 256MB - Flash
3	Interface Cards	Interface Speed	Up to multiple OC-3
		Interface Media Flexibility	Modular router must support many interface types

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
		Queuing Properties	Multiple Queuing strategies
		Online Insertion & Removal	Required
4	Operating System	Type (Modular)	Preferred (See Implementation Guidance)
		Features Supported	Required: Routing, Bridging, Switching
		Routing Protocols	Required: BGPv4, OSPF, Preferred: EIGRP (See Evaluation Criteria)
		Quality of Service	Required: including shaping and policing
		Protocols Supported	Required: MPLS, IPv4, IPv6, 802.1Q, GRE, IPSEC, GDOI
		Network Management	Required: SNMPv1 thru 3, SSH, SSL, IP-SLA, Syslog, Traps (See evaluation criteria for IP Flow export)
5	WAN Encryption	FIPS 140-2 Certification	Required: Complete, or in process. (See Implementation Guidance)
		Throughput	Required: >= 5Gbps (Inbound/Outbound Aggregate) (See Evaluation Criteria)
		Hardware vs Software	Required: Hardware
		Latency	Required: <=100usec
		Performed using Encapsulation(Tunneling) vs. Payload	Payload preferred, (See Implementation Guidance)
		Supported Connection Count	Required: >=2000 encrypted tunnels
		Interface Type	Required: Encryption Supported on all interface types
6	Platform Supportability	Technical Support	required
		Parts Replacement	required
7	Platform Maturity	Operating System Maturity	required

ID	Primary Attribute	Secondary Attribute	Specification
		Hardware Maturity	required
		Quality Assurance Certification	required

2.3 WIDE AREA NETWORK

2.3.1 METRO DATA CENTER TO BACKBONE

Specifications identifying National Data Center to VA Backbone connectivity.

ID	Primary Attribute	Secondary Attribute	Specification
1	WAN	Latency	Currently < 60ms
		Transport Method	MPLS Preferred
		Reliability/SLA/Packet Loss	(See Appendix E)
		Path Diversity (Includes Local Loop)	Required
		Carrier Diversity	Required: Qwest and ATT are the carriers of choice based on the Networx Contract
		Capacity	Minimum OC-3 per carrier
		Quality of Service	TBD
		Networx Carriers	Qwest and ATT
		Traffic Analysis / Probes	Analyzed monthly by Capacity Planning Team at the NSOC

2.3.2 METRO DATA CENTER TO REGION WAN

Specifications identifying National Data Center to Region WAN connectivity.

ID	Primary Attribute	Secondary Attribute	Specification
1	WAN	Latency	Require: <= 100ms, Acceptable: <= 60ms, Prefer: <= 40ms

ID	Primary Attribute	Secondary Attribute	Specification
		Transport Method	MPLS Required
		Reliability/SLA/Packet Loss	(See Appendix E)
		Path Diversity (Includes Local Loop)	Required; including diverse LECs, and COs; or CPA as a last resort
		Carrier Diversity	Required; including diverse LECs, and COs; or CPA as a last resort
		Capacity	N+1 (dual-circuits don't exceed 50% utilization)
		Quality of Service	Required, (Priority Queuing, + >= 2 non-priority queues, + default)
		Networx Carriers	Qwest and ATT
		Traffic Analysis / Probes	Analyzed monthly by Capacity Planning Team at the NSOC

2.3.3 MEDICAL CENTER TO REGION WAN

Specifications identifying Medical Center to Region WAN connectivity.

ID	Primary Attribute	Secondary Attribute	Specification
1	WAN	Latency	Require: <= 100ms, Acceptable: <= 60ms, Prefer: <= 40ms
		Transport Method	Option #1: MPLS/PTP Hybrid, (See Implementation Guidance) <REGION 2&3> Option #2: MPLS Required, (See Implementation Guidance) <REGION 1&4>
		Reliability/SLA/Packet Loss	(See Appendix E)
		Path Diversity (Includes Local Loop)	Required (direct patient care/continued business operations); Preferred (non patient care) (See Explanation of Standard)
		Carrier Diversity	Required when circuits are MPLS.
		Capacity	N+1 (dual-circuits don't exceed 50% utilization)
		Quality of Service	Required, (Priority Queuing, + >= 2 non-priority queues, +

ID	Primary Attribute	Secondary Attribute	Specification
			default)
		Networx Carriers	Required
		Traffic Analysis / Probes	Required

2.3.4 MEDICAL CENTER BRANCH OFFICE TO REGION WAN

Specifications identifying Medical Center Branch Office (OPC, CBOC, Admin Offices) connectivity to Region WAN.

ID	Primary Attribute	Secondary Attribute	Specification
1	WAN	Latency	Require: <= 100ms, Acceptable: <= 60ms, Prefer: <= 40ms
		Transport Method	**See Implementation Guidance:** Option #1: Direct Pt-to-Pt Option #2: Metro Ethernet Option #3: MPLS
		Reliability/SLA/Packet Loss	(See Appendix E)
		Path Diversity (Includes Local Loop)	Required for Critical Facilities (direct patient care/continued business operations), otherwise Path diversity is preferred
		Carrier Diversity	Not Required
		Capacity	N+1 Required for Critical Facilities, otherwise preferred and determined by business needs
		Quality of Service	Required, (Priority Queuing, + >= 2 non-priority queues, + default)
		Networx Carriers	Required
		Traffic Analysis / Probes	Required

2.4 WAN ENCRYPTION

Identifies WAN Encryption requirements for Data Center and Medical Center.

2.4.1 DATA CENTER

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
1	Encryption	FIPS 140-2 Validation	Complete, or in process. (See Implementation Guidance)
		Throughput	>= 10 Gbps Full Duplex (See Evaluation Criteria)
		Hardware vs. Software	Hardware
		Latency Introduced	<= 100µs
		Performed using Encapsulation(Tunneling) vs. Payload	Payload preferred, (See Implementation Guidance)
		Supported Connection Count	>= 10,000
		Cryptography	AES-256 bit
		Jumbo Frame Support	Required
		Interface Type	Carrier Metro Ethernet, Dark-Fiber, and Ethernet over Sonet
		Bypass Capability	Required
2	Chassis	Power Supply Redundancy	Required
		In-Band Management	Required
		Out of Band Management	Recommended

2.4.2 MEDICAL CENTER

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*

ID	Primary Attribute	Secondary Attribute	Specification
1	Encryption	FIPS 140-2 Validation	Complete, or in process. (See Implementation Guidance)
		Throughput	>= 5 Gbps Full Duplex (See Evaluation Criteria)
		Hardware vs. Software	Hardware
		Latency Introduced	<= 100µs
		Performed using Encapsulation(Tunneling) vs. Payload	Payload preferred, (See Implementation Guidance)
		Supported Connection Count	>= 2,000 encrypted tunnels
		Cryptography	AES-256 bit, 3DES, IPSec
		Jumbo Frame Support	Required
		Interface Type	Required: Encryption supported on all interface types
		Bypass Capability	Required
2	Chassis	Power Supply Redundancy	Required
		In-Band Management	Required
		Out of Band Management	Recommended

2.5 WAN ACCELERATION

Specifications for WAN Acceleration in the Data Center.

2.5.1 DATA CENTER

ID	Primary Attribute	Secondary Attribute	Specification
1	WAN Acceleration	Interface Type	Copper or Fiber (RJ45 or LC)
		Capacity	See Implementation Guidance
		Implementation (inline vs.	

ID	Primary Attribute	Secondary Attribute	Specification
		redirection)	
		Redundancy	Preferred
		Traffic Types Supported	CIFS, MAPI, MAPI NSPI, HTTP, HTTPS, FTP, MS-SQL, Oracle SQL
		Centralized Management and Reporting	Required
		Connection Management / Visibility	Network monitoring including support for AAA and SNMP is required
		Effectiveness (Application Acceleration, compression, Auto-Discovery)	Greater than 80% data reduction is desired

2.5.2 MEDICAL CENTER

Specifications for WAN Acceleration in the Medical Center

ID	Primary Attribute	Secondary Attribute	Specification
1	WAN Acceleration	Interface Type	Copper or Fiber (RJ45 or LC)
		Capacity	See Implementation Guidance
		Implementation (inline vs. redirection)	
		Redundancy	Preferred
		Traffic Types Supported	CIFS, MAPI, MAPI NSPI, HTTP, HTTPS, FTP, MS-SQL, Oracle SQL
		Centralized Management and Reporting	Required
		Connection Management / Visibility	Network monitoring including support for AAA and SNMP is required
		Effectiveness (Application Acceleration, compression, Auto-Discovery)	Greater than 80% data reduction is desired

3 SUPPORTING DETAILS FOR STANDARDS

3.1 CLASS A ROUTER – OC3(QTY:4) AND HIGHER

3.1.1 CHASSIS

CHASSIS STANDARD

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
1	Chassis	Type	Required: Modular
		Throughput	Backplane performance of >= 15 Millions packets per second
		Packet Processor Redundancy	Required
		Control Plane Redundancy	Required
		Cooling Redundancy	Required: May be internal to power supplies
		Power Supply Redundancy	Required
		Front-Back Airflow	Required
		Online Insertion & Removal	Required

EXPLANATION OF STANDARD

The class "A" router is for use in situations where there is a very high volume of traffic and where any service interruption is unacceptable. It is envisioned that this router would be installed at Data Centers and major network aggregation points within the VA and considered to be at the Core Layer. This type is often referred to as a carrier class router.

A modular chassis will be required in order to support redundant power as well as redundant route processors for required High Availability.

Due to the lack of data to support actual throughput required we have utilized the throughput capabilities of current architectures being utilized today.

A redundant packet processor is an essential component to a high-availability data network which provides non-stop forwarding and state-full failover during a negative event. Control Plane Redundancy provides the ability to recover from a negative event targeting the router/switch control plane. Additionally a redundant control plane

provides the ability to perform in-service software upgrades, take advantage of nonstop forwarding and state-full switchover to a redundant processor.
During normal operation, electrical components of a switching system product heat which is necessary to be dissipated to maintain proper operation. Many implementations of switching systems have a system protection feature that will shut down a system if it overheats. To satisfy a high availability system it is critical to include N+1 redundancy for both cooling and system power.

Front-Back Airflow is a desirable feature to a core network switch that will reside in a data center design and will allow for hot-cold aisle deployment and contribute to more efficient cooling and increased energy efficiency.

Through the lifetime of a system it is occasionally necessary to replace failed components or to upgrade others with more memory or with a next generation component. The ability to replace such component while the system is fully operation with near zero interruption to the normal operation of the system is required in a high availability environment. To facilitate this requirement the chassis must have the capability to support online insertion and removal of "hot-pluggable" components.

EVALUATION FACTORS

- Stability: Will be implemented in a Healthcare environment
- Slot count of Chassis and Port count of Modules
- Packet Switching performance
- WAN Protocols and Features supported
- Experience VA currently has with solution

IMPLEMENTATION GUIDANCE

None

3.1.2 PACKET PROCESSOR

STANDARD

ID	***Secondary Attribute***	***Specification***
2	Type (upgradable)	Required (not integral to chassis)
	Packet Processor Redundancy	Required
	Layer 3 Routing Throughput (PPS)	>= 15 Million packets per second

	Online Insertion & Removal	Required
	Memory (DRAM, Flash)	Upgradeable - Volatile >= 2GB, Non-Volatile >= 1GB

EXPLANATION OF STANDARD

A modular and upgradable packet processor is desirable to allow for the leveraging of new technologies while protecting the investment in purchased interfaces and chassis.

At the time of the writing of this document, specific data identifying the performance criteria for the applications supported by the Routing Platform was not available; therefore, the authors utilized switching performance data from existing architectures in place today. The throughput of a packet processor, while largely theoretical, does provide a loose scale by which one system can be measured against another.

The capability of a packet processor to allow of online insertion and removal is an essential component to a high-availability network design to allow for in-service technology upgrades and failed component replacement without interrupting critical traffic flows.

EVALUATION FACTORS

- For throughput and memory attributes, the higher the number, the better.

IMPLEMENTATION GUIDANCE

None

3.1.3 INTERFACE CARDS

STANDARD

ID	*Secondary Attribute*	*Specification*
3	Interface Speed	Up to 10Gbps
	Interface Media Flexibility	Required (from T-1 to 10Gbps interfaces) T-1, channelized T-1, DS-3, channelized DS-3, OC-3 to OC12, OC-3 to OC-12 Packet over SONET, 10Mbps to 10Gbps Ethernet, at a minimum. (see Evaluation Factors)
	Queuing Properties	Required: see 3.1.4 Operating System
	Online Insertion & Removal	Required

EXPLANATION OF STANDARD

Interface speeds up to 10 Gbps will need to be supported in a Class A (Carrier Class) Router. The Class A router will reside primarily in the National Data Centers and locations where high volumes of traffic will be routed within the VA.

Interface Media flexibility is important. As requirements change or Carrier Services change it is important to be able to adapt. Today the VA utilizes the above specified interfaces and are required to be supported by the Class A routing platform.

Interface cards are required to support queuing mechanisms instituted by the platforms operating system. See section 3.1.4 for further discussion on queuing.

Through the lifetime of a system it is occasionally necessary to replace failed components or to upgrade others with more memory or with a next generation component. The ability to replace such component while the system is fully operation with near zero interruption to the normal operation of the system is required in a high availability environment. To facilitate this requirement the chassis must have the capability to support online insertion and removal of “hot-pluggable” components.

EVALUATION FACTORS

- For Interface Media Flexibility – in order to cover all eventualities a very wide range of interfaces is desired.

IMPLEMENTATION GUIDANCE

None

3.1.4 OPERATING SYSTEM

STANDARD

ID	Secondary Attribute	Specification
4	Type (Modular)	Preferred (See Implementation Guidance)
	Features Supported	Required: Routing, Bridging, Switching
	Routing Protocols	Required: BGPv4, OSPF, Preferred: EIGRP (See Evaluation Criteria)
	Queuing/Quality of Service	Required: including shaping and policing
	Protocols Supported	Required: MPLS, IPv4, IPv6, 802.1Q, GRE, IPSEC, GDOI
	Network Management	Required: SNMPv2c and v3, SSH, SSL, IP-SLA, Syslog, SNMP Traps, Centralized AAA (see evaluation criteria for IP Flow export)

EXPLANATION OF STANDARD

A modular Operating System is preferred due to its ability to upgrade individual components of the OS. This reinforces the high availability design model.

The routing platform will be required to support features to include Routing, Bridging, and Switching for flexibility in design for HA environments.

The two routing protocols used within the Department of Veterans Affairs are EIGRP and BGPv4. EIGRP is highly preferred in order to take advantage of existing VA expertise and to be compatible with current infrastructure deployments. OSPF is required as a standards based alternative to EIGRP for compatibility between venders.

The queuing properties demonstrate the components ability to allow packets to be en-queued for transmission on a port at a rate greater than the physical medium can support. The ability for port interfaces to have compound buffers and queues translates directly to the performance on the overall system. With compound buffers and queues it becomes possible to classify different applications and assigning appropriate priorities to those traffic flows enabling the system to queue important and time sensitive traffic in front of less important and less time sensitive traffic.

In managing the WAN infrastructure the specified protocols are required to support roles based management, configuration management, and monitoring.

EVALUATION FACTORS

- Routing Protocols - The two routing protocols used within the Department of Veterans Affairs are EIGRP and BGPv4. EIGRP is highly preferred in order to take advantage of existing VA expertise and to be compatible with current infrastructure deployments.
- A method to export IP flow information via UDP or SCTP is highly desirable. Since the current VA infrastructure is Cisco today the Netflow feature is utilized to export IP Flow information. The IETF standard is IPFIX which is based on Cisco's Netflow Version 9 implementation.

IMPLEMENTATION GUIDANCE

Modular Operating System – A Modular Operating system that permits the upgrade of code in all modules without service interruption is the goal. Code maturity will be a major consideration on whether or not it is selected. Caveats and known issues identified in manuals, customer feedback, and bug notices will be examined.

3.1.5 WAN ENCRYPTION

STANDARD

ID	Secondary Attribute	Specification
5	FIPS 140-2 Certification	Required: Complete, or in process. (See Implementation Guidance)
	Throughput	Required: >= 5Gbps (Inbound/Outbound Aggregate) (See Evaluation Criteria)
	Hardware vs Software	Required: Hardware
	Latency	Required: <=100usec
	Performed using Encapsulation(Tunneling) vs. Payload	Payload preferred, (See Implementation Guidance)
	Supported Connection Count	Required: >=2000 encrypted tunnels
	Interface Type	Required: Encryption Supported on all interface types

EXPLANATION OF STANDARD

When WAN Encryption is required for WAN circuits the encryption method must be FIPS 140-2 certified (see implementation guidance for further details).

Without current data requirements to identify the required encryption throughput the throughput has been identified using the current specifications from technology implemented in the VA today.

Encryption performed in hardware will be a requirement for high volume environments such as Data Centers and VAMC's. Encryption done in software could be acceptable for low bandwidth requirements (see implementation guidance for further details).

Latency requirements were derived from existing infrastructure components deployed in the VA today. There is not enough data to support encryption latency requirements.

Encryption using Encapsulation – Payload encryption is preferred as it preserves the packet headers that include routing and Quality of Service (QoS) parameters. This reduces management and configuration overhead.

EVALUATION FACTORS

- WAN Encryption Throughput – The higher the throughput the better.

IMPLEMENTATION GUIDANCE

FIPS 140-2 Certification - The system must be either FIPS 140-2 NIST certified or at least in stage 3 testing.

Encryption using Encapsulation – Payload encryption is preferred as it preserves the packet headers that include routing and Quality of Service (QoS) parameters. This reduces management and configuration overhead.

3.1.6 PLATFORM SUPPORTABILITY

STANDARD

ID	*Secondary Attribute*	*Specification*
5	Technical Support	Required: Phone support 7x24x365
	Parts Replacement	Required: With onsite 4 hour replacement

EXPLANATION OF STANDARD

Due to the HA requirement for a Class A router Technical Support needs to be 7x24x365 with four hour parts replacement.

EVALUATION FACTORS

- If something better than onsite 4 hour support is offered it will be considered.

IMPLEMENTATION GUIDANCE

None

3.1.7 PLATFORM MATURITY

STANDARD

ID	Secondary Attribute	Specification
6	Operating System Maturity	Required, 1 year in general production
	Hardware Maturity	Required, 1 year in general production
	Quality Assurance Certification	Employs a rigorous testing program in a laboratory environment that simulates a "real world" enterprise network. Testing of both hardware and software that verifies feature functionality and interoperability under "real world" traffic loads.

EXPLANATION OF STANDARD

Due to the critical nature of a class "A" router, it is imperative for the platform to have been in general production for a period of time in order for the platform to mature and become highly stable. Early platform adoption many times requires frequent OS upgrades due to bugs being found in hardware as well as software.

EVALUATION FACTORS

- The 1 year general production requirement allows past performance to be evaluated.
- Quality Assurance Certification programs employed by venders.

IMPLEMENTATION GUIDANCE

None

3.2 CLASS B ROUTER – DS3(QTY:4) UP TO OC3(QTY:3)

3.2.1 CHASSIS

STANDARD

ID	Secondary Attribute	Specification
1	Type (Modular vs. Static)	Modular required
	System Throughput	2 Million pps
	Packet Processor Redundancy	Preferred
	Control Plane Redundancy	Preferred
	Cooling Redundancy	Preferred
	Power Supply Redundancy	Required
	Front-Back Airflow	Preferred
	Online Insertion & Removal	Required

EXPLANATION OF STANDARD

A modular chassis will be required in order to support redundant power as well as redundant route processors for required High Availability.

Due to the lack of data to support actual throughput required we have utilized the throughput capabilities of current architectures being utilized today.

A redundant packet processor is an essential component to a high-availability data network which provides non-stop forwarding and state-full failover during a negative event. Control Plane Redundancy provides the ability to recover from a negative event targeting the router/switch control plane. Additionally a redundant control plane provides the ability to perform in-service software upgrades, take advantage of nonstop forwarding and state-full switchover to a redundant processor.

During normal operation, electrical components of a switching system product heat which is necessary to be dissipated to maintain proper operation. Many implementations of switching systems have a system protection

feature that will shut down a system if it overheats. To satisfy a high availability system it is critical to include N+1 redundancy for both cooling and system power.

Front-Back Airflow is a desirable feature to a core network switch that will reside in a data center design and will allow for hot-cold aisle deployment and contribute to more efficient cooling and increased energy efficiency.

Through the lifetime of a system it is occasionally necessary to replace failed components or to upgrade others with more memory or with a next generation component. The ability to replace such component while the system is fully operation with near zero interruption to the normal operation of the system is required in a high availability environment. To facilitate this requirement the chassis must have the capability to support online insertion and removal of "hot-pluggable" components.

EVALUATION FACTORS

- Stability: Will be implemented in a Healthcare environment
- Slot count of Chassis and Port count of Modules
- Packet Switching performance
- WAN Protocols and Features supported
- Experience VA currently has with solution

IMPLEMENTATION GUIDANCE

3.2.2 PACKET PROCESSOR

STANDARD

ID	*Secondary Attribute*	*Specification*
2	Type (upgradable)	Required
	Packet Processor Redundancy	Preferred
	Layer 3 Routing Throughput (pps)	2 Million pps
	Online Insertion & Removal	Preferred
	Memory (DRAM, Flash)	1 GB – DRAM, 256MB - Flash

EXPLANATION OF STANDARD

A modular and upgradable packet processor is desirable to allow for the leveraging of new technologies while protecting the investment in purchased interfaces and chassis.

At the time of the writing of this document, specific data identifying the performance criteria for the applications supported by the Routing platform was not available; therefore, the authors utilized switching performance data from existing architectures in place today. The throughput of a packet processor, while largely theoretical, does provide a loose scale by which one system can be measured against another.

The capability of a packet processor to allow of online insertion and removal is an essential component to a high-availability network design to allow for in-service technology upgrades and failed component replacement without interrupting critical traffic flows.

EVALUATION FACTORS

- For throughput and memory attributes, the higher the number, the better.

IMPLEMENTATION GUIDANCE

3.2.3 INTERFACE CARDS

STANDARD

ID	Secondary Attribute	Specification
3	Interface Speed	Up to multiple OC-3
	Interface Media Flexibility	Required (from T-1 to OC-3 interfaces) T-1, channelized T-1, DS-3, channelized DS-3, OC-3, OC-3 Packet over SONET, 10 Mbps to 1 Gbps Ethernet, at a minimum. (see Evaluation Factors)
	Queuing Properties	Required: see 3.1.4 Operating System
	Online Insertion & Removal	Required

EXPLANATION OF STANDARD

Interface speeds up to OC-3 will need to be supported in a Class B Router. The Class B router will reside primarily at the Distribution Layer and locations where high volumes of traffic will be routed within the VA.

Interface Media flexibility is important. As requirements change or Carrier Services change it is important to be able to adapt. Today the VA utilizes the above specified interfaces and are required to be supported by the Class A routing platform.

Interface cards are required to support queuing mechanisms instituted by the platforms operating system. See section 3.2.4 for further discussion on queuing.

Through the lifetime of a system it is occasionally necessary to replace failed components or to upgrade others with more memory or with a next generation component. The ability to replace such component while the system is fully operation with near zero interruption to the normal operation of the system is required in a high availability environment. To facilitate this requirement the chassis must have the capability to support online insertion and removal of “hot-pluggable” components.

EVALUATION FACTORS

- For Interface Media Flexibility – in order to cover all eventualities a very wide range of interfaces is desired.

IMPLEMENTATION GUIDANCE

3.2.4 OPERATING SYSTEM

STANDARD

ID	*Secondary Attribute*	*Specification*
4	Type (Modular)	Preferred (See Implementation Guidance)
	Features Supported	Required: Routing, Bridging, Switching
	Routing Protocols	Required: BGPv4, OSPF, Preferred: EIGRP (See Evaluation Criteria)
	Quality of Service	Required: including shaping and policing
	Protocols Supported	Required: MPLS, IPv4, IPv6, 802.1Q, GRE, IPSEC, GDOI
	Network Management	Required: SNMPv2c and v3, SSH, SSL, IP-SLA, Syslog, SNMP Traps, Centralized AAA (see evaluation criteria for IP Flow export)

EXPLANATION OF STANDARD

A modular Operating System is preferred due to its ability to upgrade individual components of the OS. This reinforces the high availability design model.

The routing platform will be required to support features to include Routing, Bridging, and Switching for flexibility in design for HA environments.

The two routing protocols used within the Department of Veterans Affairs are EIGRP and BGPv4. EIGRP is highly preferred in order to take advantage of existing VA expertise and to be compatible with current infrastructure deployments. OSPF is required as a standards based alternative to EIGRP for compatibility between venders.

The queuing properties demonstrate the components ability to allow packets to be en-queued for transmission on a port at a rate greater than the physical medium can support. The ability for port interfaces to have compound buffers and queues translates directly to the performance on the overall system. With compound buffers and queues it becomes possible to classify different applications and assigning appropriate priorities to those traffic flows enabling the system to queue important and time sensitive traffic in front of less important and less time sensitive traffic.

In managing the WAN infrastructure the specified protocols are required to support roles based management, configuration management, and monitoring.

EVALUATION FACTORS

- Routing Protocols - The two routing protocols used within the Department of Veterans Affairs are EIGRP and BGPv4. EIGRP is highly preferred in order to take advantage of existing VA expertise and to be compatible with current infrastructure deployments.
- A method to export IP flow information via UDP or SCTP is highly desirable. Since the current VA infrastructure is Cisco today the Netflow feature is utilized to export IP Flow information. The IETF standard is IPFIX which is based on Cisco's Netflow Version 9 implementation

IMPLEMENTATION GUIDANCE

Modular Operating System – A Modular Operating system that permits the upgrade of code in all modules without service interruption is the goal. Code maturity will be a major consideration on whether or not it is selected. Caveats and known issues identified in manuals, customer feedback, and bug notices will be examined.

3.2.5 WAN ENCRYPTION

STANDARD

ID	Secondary Attribute	Specification
5	FIPS 140-2 Certification	Required: Complete, or in process. (See Implementation Guidance)
	Throughput	Required: >= 900Mbps (Inbound/Outbound Aggregate) (See Evaluation Criteria)
	Hardware vs Software	Required: Hardware
	Latency	Required: <=100usec
	Performed using Encapsulation(Tunneling) vs. Payload	Payload preferred, (See Implementation Guidance)
	Supported Connection Count	Required: >=2000 encrypted tunnels
	Interface Type	Required: Encryption Supported on all interface types

EXPLANATION OF STANDARD

When WAN Encryption is required for WAN circuits the encryption method must be FIPS 140-2 certified (see implementation guidance for further details).

Without current data requirements to identify the required encryption throughput the throughput has been identified using the current specifications from technology implemented in the VA today.

Encryption performed in hardware will be a requirement for high volume environments such as Data Centers and VAMC's. Encryption done in software could be acceptable for low bandwidth requirements (see implementation guidance for further details).

Latency requirements were derived from existing infrastructure components deployed in the VA today. There is not enough data to support encryption latency requirements.

Encryption using Encapsulation – Payload encryption is preferred as it preserves the packet headers that include routing and Quality of Service (QoS) parameters. This reduces management and configuration overhead.

EVALUATION FACTORS

- WAN Encryption Throughput – The higher the throughput the better.

IMPLEMENTATION GUIDANCE

FIPS 140-2 Certification - The system must be either FIPS 140-2 NIST certified or at least in stage 3 testing.

Encryption using Encapsulation – Payload encryption is preferred as it preserves the packet headers that include routing and Quality of Service (QoS) parameters. This reduces management and configuration overhead.

3.2.6 PLATFORM SUPPORTABILITY

STANDARD

ID	Secondary Attribute	Specification
5	Technical Support	Required: Phone support 7x24x365
	Parts Replacement	Required: With onsite 4 hour replacement

EXPLANATION OF STANDARD

Due to the HA requirement for a Class B router Technical Support needs to be 7x24x365 with four hour parts replacement.

EVALUATION FACTORS

- If something better than onsite 4 hour support is offered it will be considered.

IMPLEMENTATION GUIDANCE

3.2.7 PLATFORM MATURITY

STANDARD

ID	Secondary Attribute	Specification
6	Operating System Maturity	required
	Hardware Maturity	required
	Quality Assurance Certification	required

EXPLANATION OF STANDARD

Due to the critical nature of a Class "B" router, it is imperative for the platform to have been in general production for a period of time in order for the platform to mature and become highly stable. Early platform adoption many times requires frequent OS upgrades due to bugs being found in hardware as well as software.

EVALUATION FACTORS

- The 1 year general production requirement allows past performance to be evaluated.
- Quality Assurance Certification programs employed by venders.

IMPLEMENTATION GUIDANCE

3.3 WIDE AREA NETWORK

3.3.1 METRO DATA CENTER TO BACKBONE

STANDARD

ID	Secondary Attribute	Specification
1	Latency	Currently < 60ms
	Transport Method	MPLS Preferred
	Path Diversity (Includes Local Loop)	Required

	Carrier Diversity	Qwest and ATT are the carriers of choice based on the Networx Contract
	Capacity	Minimum OC-3 per carrier
	Quality of Service	TBD
	Networx Carriers	Qwest and ATT
	Traffic Analysis	Analyzed monthly by Capacity Planning Team at the NSOC

EXPLANATION OF STANDARD

A 2-port OC-3 adaptor will be used to terminate the OC-3 circuits from AT&T and Sprint on the One-VA distribution routers. Each AS will have two exit points out of the Region via a circuit to each MPLS network. Equal cost routing will take place at the distribution nodes and traffic will utilize and load share between both MPLS connections.

Each One-VA distribution router will have an External BGP (eBGP) peer with both MPLS networks (a peer with AT&T AS 7018 and a peer with Qwest AS 209). The routers will also have an internal BGP (iBGP) peer with each other to exchange routing information. The routers will be configured to forward only the networks that belong to that region. This will be accomplished with the use of route maps and prefix lists defining the prefixes belonging to a region. The routes will be advertised from each distribution node to each of the carrier MPLS networks with equal metrics per demarc location. Routes will be advertised back into other VA regions from both MPLS networks.

The routing architecture will make use of route maps to set metrics and to tag routes with specific BGP communities. The current ATM routing topology uses the Multi-Exit Discriminator (MED) attribute to set metrics. The MED attribute tells external neighbors about the preferred path into an AS when there are multiple entry points into the AS. The exit point with the lowest metric is preferred. If a MED is received over an external BGP link, it is propagated over internal links to other BGP speaking routers within the AS. MED is a non-transitive attribute and is not passed from the provider networks; therefore, along with setting MEDs using routes maps, routes will also be tagged with specific communities. The communities are a transitive attribute and will be used to mark or tag specific subnets. All routes inbound from the MPLS networks to a region will have a specific community associated with them. This will allow the routes to be identified and metrics set according to specific route policies. The router configurations will set metrics inbound and outbound for routes using communities. The VA Regions will be required to split their networks so one-half of their routes prefer one distribution node while the remaining routes will prefer the second distribution node.

Each distribution router will have two WAN connections and will receive all routes on each; however, BGP, by default, uses the best path algorithm to install the one best path in the IP routing table to use for traffic forwarding. If BGP multipath is enabled using the *maximum-paths* configuration command and the eBGP paths are learned from the same neighboring AS, instead of picking one best path, multiple paths are installed in the route table. However, the One-VA distribution routers will receive two equal eBGP paths from different neighboring AS numbers (AS 209 for Qwest and AS 7018 for AT&T). BGP will not install the desired equal cost routes based on the fact that the routes are being sent by different AS. In order to overcome this “limitation” and accomplish equal cost routing at each distribution node, the routing configuration will make use of a new BGP command: *bgp best path as-path multpath-relax*. Based on lab testing conducted by the engineering team, this configuration

command works by installing equal paths from differing AS into the Routing Information Base (RIB). This will allow traffic to effectively load share between the MPLS networks. This works with the caveat that the router BGP configuration command *bgp deterministic-med* is not configured.

Default Route and Internet Gateway Tunnel

Each tunnel will be built from the loopback0 address of the distribution router to a unique loopback1 address on one of the gateway routers in each location. The loopback1 addresses will be independent of the loopback0 addresses used for the gateway routers administration. By using a separate loopback address at the gateways recovering the tunnels in the case of a catastrophic failure of the primary tunnel endpoint router hardware can be accomplished by rebuilding the tunnels to the remaining router in service using the loopback1 information from the failed router.

Since the tunnel overlay is already engineered and established it can be used for IPv6 routing. Once the decision to enable IPv6 in a dual protocol stack routing configuration is made, the BGP peers to the gateway locations will be modified to allow the IPv4 default gateway as well as the full IPv6 routing table to pass over the tunnel peers. Once the MPLS carriers can support the IPv6 protocol, the tunnels will be reconfigured to allow only the default route for IPv4 to pass over them. The default IPv6 route will also be added to the tunnel design if all 4 gateway locations can support that configuration.

Fail-over Design

The tunnel and default routing failover design was engineered to provide for failover if the default route for a gateway location is no longer received. If the route is not received by the preferred gateway, the router will no longer announce a default route to the distribution node. Since the Distribution nodes are split between gateway locations, the other regional distribution node will continue to receive the default route and outbound traffic will shift to that distribution node.

In the case of a distribution node's loss of both MPLS providers the tunnel would by default attempt to establish through the other distribution point. Since this is an undesirable failover situation the regions BGP peer between the two distribution nodes will filter out the loopback1 gateway routes it learns from the MPLS carriers. With these routes filtered if a distribution node does lose both carriers the tunnel will fail and the remaining default route will remain as the only default route for the region.

EVALUATION FACTORS

-

IMPLEMENTATION GUIDANCE

3.3.2 METRO DATA CENTER TO REGION WAN

STANDARD

ID	*Secondary Attribute*	*Specification*
1	Latency	Require: <= 100ms, Acceptable: <= 60ms, Prefer: <= 40ms
2	Transport Method	MPLS Required
3	Reliability/SLA/Packet Loss	(See Appendix E)
4	Path Diversity (Includes Local Loop)	Required; including diverse LECs, and COs; or CPA as a last resort
5	Carrier Diversity	Required
6	Capacity	N+1 (dual-circuits don't exceed 50% utilization)
7	Quality of Service	Required, (Priority Queuing, + >= 2 non-priority queues, + default)
8	Networx Carriers	Required
9	Traffic Analysis / Probes	Required

EXPLANATION OF STANDARD

The Networx contract stipulates less than 100ms of latency. It is preferred to achieve less than 60ms of latency on the WAN due to observed performance on existing networks with a maximum round trip of 60ms. The requirement for 40ms is an un-verified assumption of a VistA requirement.

Data Center connectivity to Region WAN will be MPLS assuming Carrier PE node location to the Data Center can support application performance requirements. With an MPLS network the technology lends itself to physical media diversity.

Reliability/SLA/Packet Loss has been pulled from the Networx contract and is included below and applies to their MPLS Service offering.

Carrier diversity is required to protect against a catastrophic carrier network outage. Extra attention to ensure path diversity would be required. To ensure physical path diversity in a multi carrier design, the carriers must work together to assure the paths are in fact diverse. Physical path diversity may prove to be difficult to maintain in a multi carrier design due to carrier reroutes during carrier outages. Physical path redundancy includes local loop including diverse Carrier Central Offices for the Local Exchange Carrier and diverse Campus Fiber paths with physical separation of fiber paths of at least 25 feet.

N+1 capacity allows for survivability of a circuit failure without impacting performance.

Quality of Service (QoS) is limited to the capabilities offered by the MPLS providers on the Networx Contract. Qwest and AT&T both support four QoS queues.

The GSA Networx Contract identifies the Telecommunications Carriers to be utilized. Primary MPLS carrier will be AT&T and the secondary carrier will be Qwest.

Traffic Analysis will be required for management, support, and capacity planning. There are multiple methods in implementing a traffic analysis solution. The traffic analysis solution will be impacted by Data Center design.

EVALUATION FACTORS

- Latency (Lower is better)
- QoS, more queues are better

IMPLEMENTATION GUIDANCE

3.3.3 MEDICAL CENTER TO REGION WAN

STANDARD

ID	***Secondary Attribute***	***Specification***
1	Latency	Require: <= 100ms, Acceptable: <= 60ms, Prefer: <= 40ms
2	Transport Method	Option #1: MPLS/PTP Hybrid, (See Implementation Guidance) <REGION 2&3> Option #2: MPLS Required, (See Implementation Guidance) <REGION 1&4>
3	Reliability/SLA/Packet Loss	See Appendix E
4	Path Diversity (Includes Local Loop)	Required; including diverse LECs, and COs; or CPA as a last resort
5	LD Carrier Diversity	Required when circuits are MPLS.
6	Capacity	N+1 (dual-circuits don't exceed 50% utilization)
7	Quality of Service	Required, (Priority Queuing, + >= 2 non-priority queues, + default)
8	Networx Carriers	Required
9	Traffic Analysis / Probes	Required

EXPLANATION OF STANDARD

The Networx contract stipulates less than 100ms of latency. It is preferred to achieve less than 60ms of latency on the WAN due to observed performance on existing networks with a maximum round trip of 60ms. The requirement for 40ms is an un-verified assumption of a VistA requirement.

Where feasible path diversity will be required for Medical Center connectivity to a Region WAN or National Data Center.

Carrier diversity is required to protect against a catastrophic carrier network outage. Extra attention to ensure path diversity would be required. To ensure physical path diversity in a multi carrier design, the carriers must work together to assure the paths are in fact diverse. Physical path diversity may prove to be difficult to maintain in a multi carrier design due to carrier reroutes during carrier outages. Physical path redundancy includes local loop including diverse Carrier Central Offices for the Local Exchange Carrier and diverse Campus Fiber paths with physical separation of fiber paths of at least 25 feet.

Capacity needs to be able to survive a circuit failure without impacting performance.

EVALUATION FACTORS

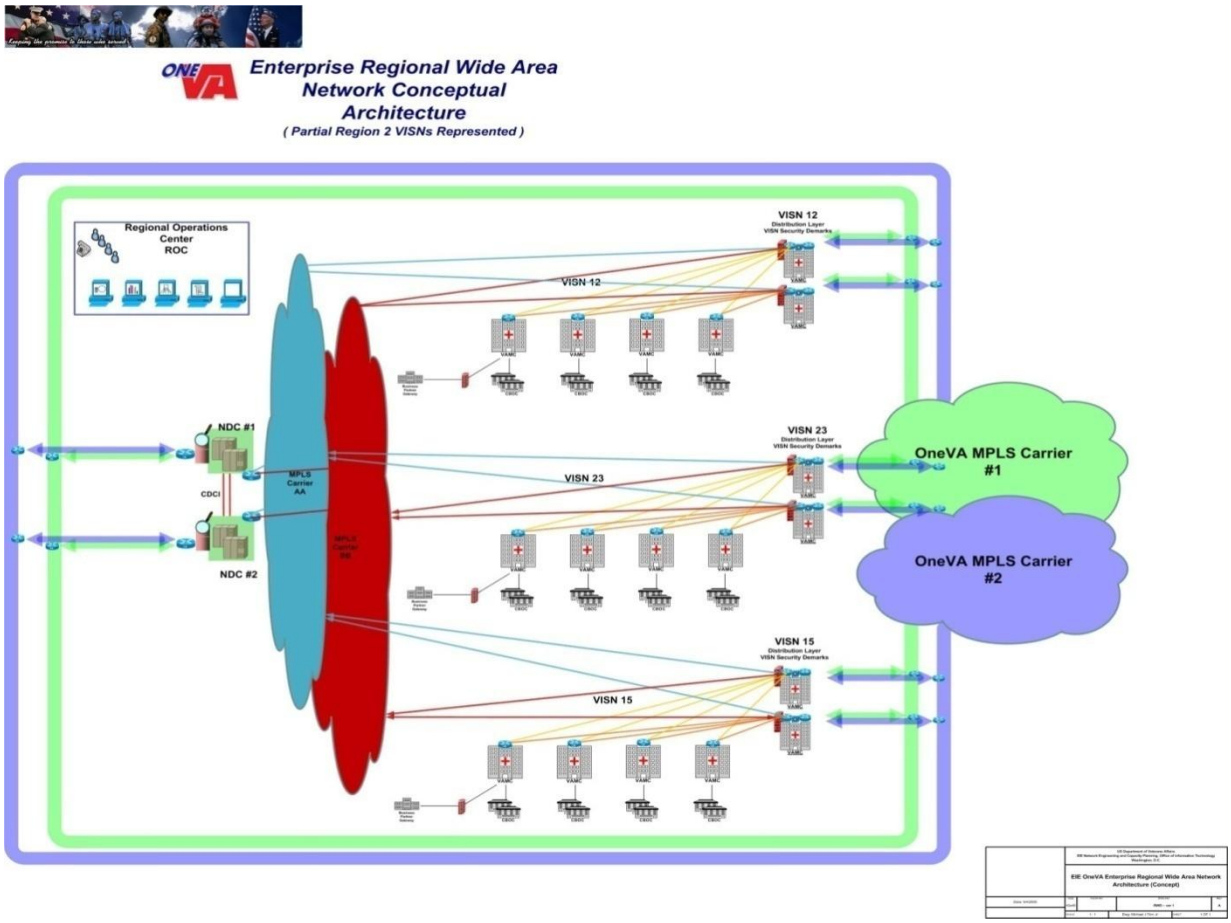
- Latency (Lower is better)
- QoS, more queues are better

IMPLEMENTATION GUIDANCE

Option #1 for VISNs within Regions 2 and 3 will leverage the performance, additional QoS queues, and security offered by Point-To-Point (PTP) circuits within a VISN's boundaries, and the cost saving associated MPLS over longer distances to the National Data Center (NDC) facilities. Specifically, within the VISN, option #1 calls for one full-line rate PTP DS3 circuit from each of the VISN's non-demark facilities to each demark facilities within the VISN (in most cases this means two DS3 will be installed). The Networx vendor shall ensure the two PTP DS3s are path-diverse from each non-demark facility to each demark facility; it is assumed where financially prudent that physical diverse entry paths will be built-out where not already available. Industry best practices leveraging Differentiated Services Code Point (DSCP) shall be implemented to ensure a viable Voice, Video, and Data Quality of Service (QoS) solution is provided within each VISN.

Traffic flow between facilities within Region 2 or 3 and the NDC will be facilitated with carrier-redundant MPLS connections at each of the VISN's demark locations. At each VISN demark two routers will be installed, one for each carrier. Each Region 2 and 3 NDC will also have associated carrier-redundant connections to both providers MPLS networks. Specifically, to ensure maximum up-time, each VISN demark facility will have connections to both Networx provider's MPLS networks, and each metro data center in both regions will also have connections into both providers. For scalability purposes, initial expectations for CE-to-PE connections are OC-3 connections for demark facility-to-provider CE-to-PE connections, and OC-12 for NDC-to-provider CE-to-PE connections.

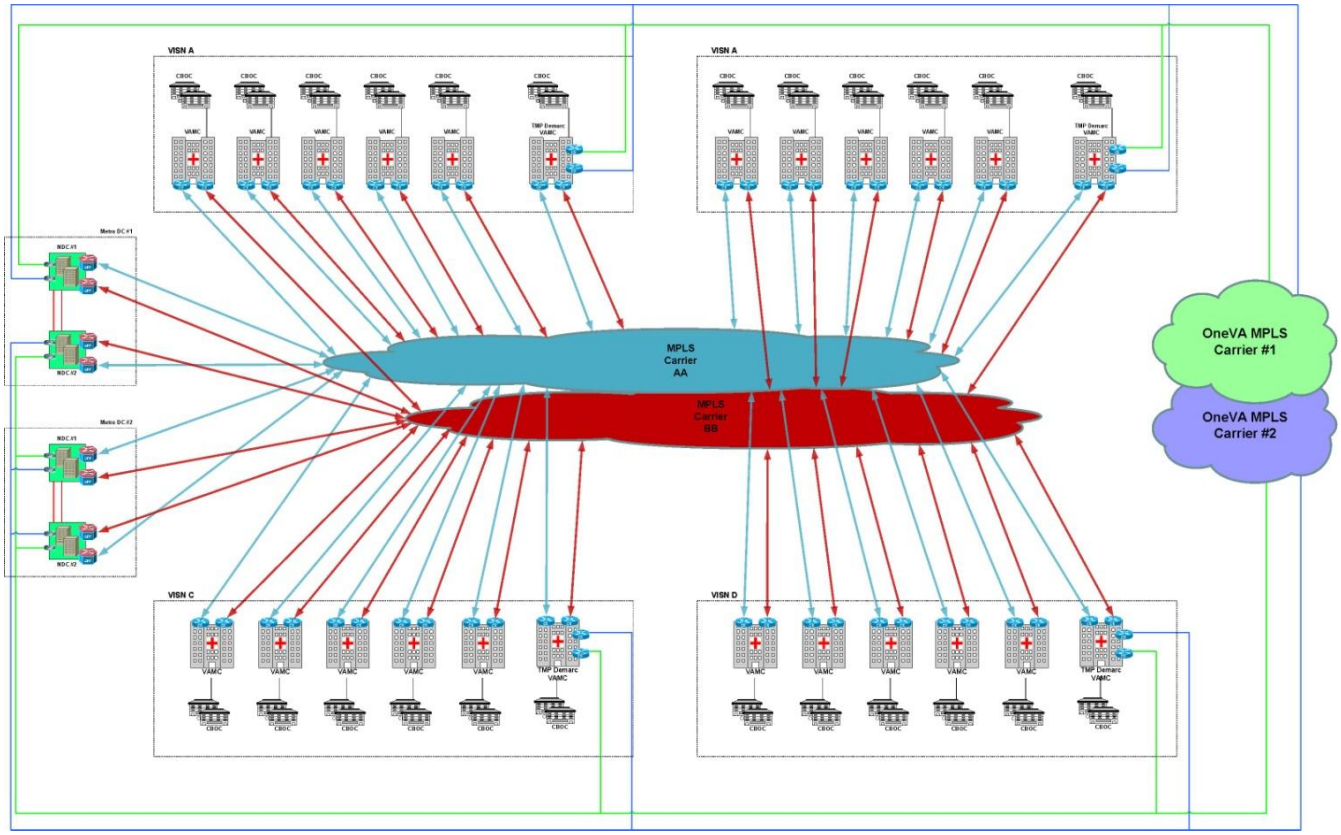
The diagram provided below is included as an example of this offering.



Option #2 for VISNs within Regions 1 and 4 will consist of redundant connections (2) to two Networx vendor provided MPLS networks (VRF's) from each Medical Center. The total WAN bandwidth capacity to the Medical Center and Datacenter facilities shall be N+1 to provide no degradation in service in the event of one circuit failure. Termination of each MPLS circuit shall be made to redundant router equipment. The Networx vendor shall ensure the two MPLS circuits are path-diverse from each non-demark facility to each demark facility; it is assumed where financially prudent that physical diverse entry paths will be built-out where not already available. The two Med Center MPLS CE-to-PE circuits will either be DS-3 or OC-3 depending on the bandwidth capacity requirements of the facility. The Datacenter MPLS CE-to-PE circuits will be OC-12.

The intent of this design is to utilize both MPLS carrier networks as redundant equal cost paths for all traffic within each Region. This includes VAMC to Datacenter and VAMC to VAMC. Industry best practices leveraging Differentiated Services Code Point (DSCP) shall be implemented to ensure a viable Voice, Video, and Data Quality of Service (QoS) solution is provided within each VISN/Region.

The diagram provided below is included as an example of this offering.


VISN A
VISN A
Metro DC #1
Metro DC #2
MPLS
Carrier
AA
MPLS
Carrier
BB
OneVA MPLS
Carrier #1
OneVA MPLS
Carrier #2
VISN C
VISN D

3.3.4 MEDICAL CENTER BRANCH OFFICE TO REGION WAN

STANDARD

ID	*Secondary Attribute*	*Specification*
1	Latency	Require: <= 100ms, Acceptable: <= 60ms, Prefer: <= 40ms
2	Transport Method	**See Implementation Guidance:** Option #1: Direct Pt-to-Pt Option #2: Metro Ethernet Option #3: MPLS
3	Reliability/SLA/Packet Loss	(See Appendix E)
4	Path Diversity (Includes Local Loop)	Required (direct patient care/continued business operations); Preferred (non patient care) (See Explanation of Standard)
5	Carrier Diversity	Not Required
6	Capacity	See Implementation guidance
7	Quality of Service	Required, (Priority Queuing, + >= 2 non-priority queues, + default)
8	Networx Carriers	Required
9	Traffic Analysis / Probes	Required

EXPLANATION OF STANDARD

The Networx contract stipulates less than 100ms of latency. It is preferred to achieve less than 60ms of latency on the WAN due to observed performance on existing networks with a maximum round trip of 60ms. The requirement for 40ms is an un-verified assumption of a VistA requirement.

Carrier Services available today and in use by the VA consist of dedicated Point to Point Circuits, Metro Ethernet/Dark Fiber, and MPLS. See implementation guide for further details.

Reliability/SLA/Packet Loss has been pulled from the Networx contract and is included below and applies to their MPLS Service offering.

Where feasible path diversity will be required for direct patient care facilities or facilities that have been deemed critical to continued business operations.

Carrier diversity where required protects against a catastrophic carrier network outage. Extra attention to ensure path diversity would be required. To ensure physical path diversity in a multi carrier design, the carriers must work together to assure the paths are in fact diverse. Physical path diversity may prove to be difficult to maintain in a multi carrier design due to carrier reroutes during carrier outages. Physical path redundancy includes local loop including diverse Carrier Central Offices for the Local Exchange Carrier and diverse Campus Fiber paths.

N+1 capacity allows for survivability of a circuit failure without impacting performance. N+1 is required for direct patient care facilities or where business needs dictate reduced service is not acceptable for business operations to continue.

Quality of Service (QoS) is limited to the capabilities offered by the MPLS providers on the Networx Contract. Qwest and AT&T both support four QoS queues. QoS capabilities for Metro Ethernet/Dark Fiber and dedicated point to point circuits will only be limited to vender transport equipment and will need to meet minimum requirements of the MPLS services available.

The GSA Networx Contract identifies the Telecommunications Carriers to be utilized. Primary MPLS carrier will be AT&T and the secondary carrier will be Qwest.

Traffic Analysis will be required for management, support, and capacity planning. There are multiple methods in implementing a traffic analysis solution. The traffic analysis solution will be impacted by Data Center design.

Capacity needs to be able to survive a circuit failure without impacting performance

EVALUATION FACTORS

- Latency (Lower is better)
- QoS, more queues are better

IMPLEMENTATION GUIDANCE

Within the Region WAN the transport method will greatly be determined by latency requirements of existing applications deployed, Carrier Services available, and density of Carrier MPLS PE Nodes.

3.4 WAN ENCRYPTION

3.4.1 DATA CENTER

STANDARD

ID	***Secondary Attribute***	***Specification***
1	FIPS 140-2 Validation	Required: Complete, or in process. (See Implementation Guidance)
	Throughput	>= 10 Gbps Full Duplex (See Evaluation Criteria)

	Hardware vs. Software	Hardware
	Latency Introduced	<= 100µs
	Performed using Encapsulation(Tunneling) vs. Payload	Payload preferred, (See Implementation Guidance)
	Supported Connection Count	>= 10,000
	Cryptography	AES-256 bit
	Jumbo Frame Support	Required
	Interface Type	Carrier Metro Ethernet, Dark-Fiber, and Ethernet over Sonet
	Bypass Capability	Required
2	Power Supply Redundancy	Required
	In-Band Management	Required
	Out of Band Management	Recommended

EXPLANATION OF STANDARD

When WAN Encryption is required between data centers, the encryption method must be FIPS 140-2 certified (see implementation guidance for further details).

Encryption throughput must satisfy high speed LAN interfaces typically found in the datacenter. Because of the expected proliferation of 10GB in the datacenter, any encryption technology procured for the data center must support 10GB at full duplex with little added latency.

At speeds of 10GB, encryption can only be performed in hardware and therefore hardware based encryption is a requirement for high volume environments such as Data Centers and VAMC's.

Latency requirements were derived from existing applications and infrastructure components deployed in the VA today. There is not enough data to support specific encryption latency requirements.

Redundant power supplies are required to satisfy the data center high availability (HA) design requirement. If the encryption device fails it should fail over to bypass mode ensuring no interruption to services or data.

Encryption using Encapsulation – Payload encryption is preferred as it preserves the packet headers that include routing and Quality of Service (QoS) parameters. This reduces management and configuration overhead.

Front-Back Airflow is a desirable feature to a core network switch that will reside in a data center design and will allow for hot-cold aisle deployment and contribute to more efficient cooling and increased energy efficiency.

EVALUATION FACTORS

- WAN Encryption Throughput – The higher the throughput the better.
- AES-256 is the preferred Cryptographic algorithm although 3DES is required to meet FIPS 140-2 criteria.
- Separate Hardware Appliances – Separating the Encryption platform from the Routing hardware is preferred. This prevents a router's IOS upgrade from voiding a product's FIPS 140-2 certification. FIPS 140-2 Certification - The system must be either FIPS 140-2 NIST certified or at least in stage 3 testing.

IMPLEMENTATION GUIDANCE

FIPS 140-2 Certification - The system must be either FIPS 140-2 NIST certified or at least in stage 3 testing.

Encryption using Encapsulation – Payload encryption is preferred as it preserves the packet headers that include routing and Quality of Service (QoS) parameters. This reduces management and configuration overhead

3.4.2 MEDICAL CENTER

STANDARD

ID	***Secondary Attribute***	***Specification***
1	FIPS 140-2 Certification	Required: Complete, or in process. (See Implementation Guidance)
	Throughput	>= 5 Gbps Full Duplex (See Evaluation Criteria)
	Hardware vs Software	Hardware
	Maximum Added Latency	<= 100µs
	Performed using Encapsulation(Tunneling) vs. Payload	Payload preferred, (See Implementation Guidance)
	Supported Connection Count	>= 2,000 encrypted tunnels
	Cryptography	AES-256 bit, 3DES, IPSec
	Bypass Capability	Required
	Jumbo Frame Support	Required

	Interface Type	Encryption Supported on all interface types
2	Power Supply Redundancy	Required
	In-Band Management	Required
	Out of Band Management	Recommended

EXPLANATION OF STANDARD

Encryption hardware used at medical centers must be FIPS 140-2 certified (see implementation guidance for further details).

Encryption hardware must be capable of connecting to all of the diffferent WAN and LAN interface types found at the medical center. Encryption throughput capabilities must satisfy the aggregate throughput of all the different interfaces found at the medical center.

Because of the volume of data processed at the medical centers, hardware encryption is a requirement at VAMC's.

Latency requirements were derived from existing applications and infrastructure components deployed in the VA today. There is not enough data to support specific encryption latency requirements.

If the encryption device fails it should fail over to bypass mode ensuring no interruption to services or data.

Encryption using Encapsulation – Payload encryption is preferred as it preserves the packet headers that include routing and Quality of Service (QoS) parameters. This reduces management and configuration overhead.

Front-Back Airflow is a desirable feature to a core network switch that will reside in a data center design and will allow for hot-cold aisle deployment and contribute to more efficient cooling and increased energy efficiency

EVALUATION FACTORS

- WAN Encryption Throughput – The higher the throughput the better.
- AES-256 is the preferred Cryptographic algorithm although 3DES is required to meet FIPS 140-2 criteria.
- Separate Hardware Appliances – Although separating encryption from the routing platform is preferred; leveraging existing router hardware by adding encryption modules will satisfy the agency's encryption requirements. However, integrated routing and encryption does create additional challenges to maintaining FIPS 140-2 certification

IMPLEMENTATION GUIDANCE

FIPS 140-2 Certification - The system must be either FIPS 140-2 NIST certified or at least in stage 3 testing.

Encryption using Encapsulation – Payload encryption is preferred as it preserves the packet headers that include routing and Quality of Service (QoS) parameters. This reduces management and configuration overhead

3.5 WAN ACCELERATION

3.5.1 DATA CENTER

STANDARD

ID	Secondary Attribute	Specification
1	Interface Type	Copper or Fiber (RJ45 or LC)
	Capacity	See Implementation Guidance
	Implementation (inline vs. redirection)	
	Redundancy	Preferred
	Traffic Types Supported	CIFS, MAPI, MAPI NSPI, HTTP, HTTPS, FTP, MS-SQL, Oracle SQL
	Centralized Management and Reporting	Required
	Connection Management / Visibility	Network monitoring including support for AAA and SNMP is required
	Effectiveness (Application Acceleration, compression, Auto-Discovery)	Greater than 80% data reduction is desired

EXPLANATION OF STANDARD

Interface type can be Copper (RJ45) or Fiber (LC/SC/ST)

The system will require having redundant connections to the network in case of an interface failure on either side of the connection.

The system is required to accelerate or optimized the following traffic types/Applications: CIFS, MAPI, MAPI NSPI, HTTP, HTTPS, FTP, MS-SQL, Oracle SQL, (Exchange 2003, 2007 is considered MAPI)

Centralized Management and reporting will be required to help with managing the solution as well as troubleshooting in an efficient manner.

Network monitoring, including support for AAA and SNMP, is required for these systems.

Effectiveness (Application Acceleration, compression, Auto-Discovery) – Greater then 80% data reduction is desired. Also, HTTP caching, separate from byte level caching is desired. . Data compression is required, normally using both layer 6 and 7 servicing of applications. Different compression algorithms can be used including LZ compression. Data Store or Byte level caching storage capability of 3 Terabytes or higher is required. This allows for a FIFO queue technique for byte cache instances to stay in the optimizer for as long as possible in case that cache instance is referenced again, which would keep it off the Wan circuit. Auto discovery allows the appliances to create optimized connections with other WAN optimizers in a dynamic fashion, removing the need to statically set up the peering between med centers and data center throughout the VA.

Redirector device –

Interface type – RJ-45 or LC (Fiber) – Both types need to be supported because both are used when connecting the Wan router to the core switches. RJ-45 are far cheaper because the failure to wire option needed for device failure is cheaper to accomplish for copper then it is for fiber (light).

Interface bypass port count – interface count needs to be able to support 4 Ethernet segments. Each segment between the WAN router and the Core switch will need a WAN and LAN port interface. A minimum of 8 ports are the current requirement.

Implementation – WAN optimization systems will be required to be put in line to optimize the traffic seen on the segments connecting the WAN routers to the LAN core switches. The redirector takes the place of the WAN optimization systems in the data centers, thereby requiring them to be in line.

Interface Capability – Interfaces are required to have the fail to wire or fail open capability in the case of power loss or system failure. Traffic then travels through the redirector without affect.

Link State Propagation -- To ensure consistency throughout networking monitoring systems, redirector appliances will be required to propagate a link state change to an opposing network device.

Centralized Management and Reporting – Required, usually by a management appliance.

Connection Management/ Visibility – Network monitoring including support for AAA and SNMP is required for these systems.

Redirection Peer – The systems redirect traffic to the cluster of WAN optimization systems for servicing so being able to detect whether the peer has failed is required.

Multiple Peer Accelerator/Optimizer Support – the redirector is required to support multiple peers which can be added to or subtracted from during production without detrimental affect.

Load Balancing Support – The redirector is required to be able to balance the load between the peer devices according to multiple algorithms, including load levels, byte caching warmth or availability or in preparations to remove or add peer devices.

Seamless Peer Additions – The redirector is required to support the addition or subtraction of peer devices to increase the load capability or to remove failed devices without detrimental affect to production environment.

Seamless Peer failover – Redirector will support failover from failed devices without negative affect to optimization process.

Ether channel support – Since we do not use this between WAN router and Core switch this is not needed.

EVALUATION FACTORS

- Ease of installation and maintenance is of prime importance in choosing a standard for WAN Optimization. Ease of maintenance is the most important factor as problems can develop with applications and traffic types that may stop users from being able to do their job.
- Visibility of connections statistics and pass through variables can help in the trouble shooting of problems being caused by the WAN optimizers. The manageability of these systems is just as important as the benefits they provide.
- Vendor support needs to be considered as evaluating factor. This can be ascertained by talking to other customers and searching the Internet for testimonial information.
- Though not a requirement, transparency mode is useful when looking at a WAN Optimization standard. This allows the IP addresses of the actual server/client will be preserved instead of the traffic being tunneled using the IP addresses of the Wan optimizers.
- WAN monitoring and reporting as well as QOS schemes can run in the same manner before the installation of WAN Optimizers. Again, this is not required because most optimizers provide a method of doing these things but it should be considered.]
- Due to the environment of the data center, it is imperative to provide a method to effectively maintain the WAN Optimizers in a safe fashion and to provide a tolerant manner to replace failed devices and increase capability without any network interruptions. Redirectors must also provide effective and thorough load balancing between the WAN optimizers. Load levels, different sized machines working together, and data warmth (up to date and easily accessible byte cache instances) must all be taken into consideration.
- Keeping the redirector separate from the routers and switches will help avoid IOS bugs that can and will materialize, will help lower the load on these switches, and will make trouble shooting optimization issues far easier.

IMPLEMENTATION GUIDANCE

Capacity will need to be determined by calculating the required concurrent number of workstation connections to the Data Center that needs acceleration. Without Exchange, recommended estimations have been identified 5 to 10 connections per workstation plus 15% growth as a guide to determine necessary capacity at the Data Center.

Many factors need to be considered while deploying and maintaining WAN optimizers. Many applications evolve or are upgraded on the client and server systems and this can have a detrimental effect on the method and effectiveness of the way the WAN optimizer operates. For instance, when MS Office was upgraded to 2007, encryption was turned on in all client systems in regards to their connections to the Exchange server. Most optimizers cannot effectively accelerate or compress encrypted or previously compressed data going across the wire. The staff that is responsible for the operations of the Optimizers must participate in all groups involved in changing profiles and applications on servers and clients. SMB signing and SMBv2 is another example of data types

that may cause issues. It will be important to use WAN optimizers that can handle these kinds of security requirements and changes.

3.5.2 MEDICAL CENTER

STANDARD

ID	***Secondary Attribute***	***Specification***
1	Interface Type	Copper or Fiber (RJ45 or LC)
	Capacity	See Implementation Guidance
	Implementation (inline vs. redirection)	
	Redundancy	Preferred
	Traffic Types Supported	CIFS, MAPI, MAPI NSPI, HTTP, HTTPS, FTP, MS-SQL, Oracle SQL
	Centralized Management and Reporting	Required
	Connection Management / Visibility	Network monitoring including support for AAA and SNMP is required
	Effectiveness (Application Acceleration, compression, Auto-Discovery)	Greater than 80% data reduction is desired

EXPLANATION OF STANDARD

Interface type can be Copper (RJ45) or Fiber (LC/SC/ST)

The system will require having redundant connections to the network in case of an interface failure on either side of the connection.

The system is required to accelerate or optimized the following traffic types/Applications: CIFS, MAPI, MAPI NSPI, HTTP, HTTPS, FTP, MS-SQL, Oracle SQL, (Exchange 2003, 2007 is considered MAPI)

Centralized Management and reporting will be required to help with managing the solution as well as troubleshooting in an efficient manner.

Network monitoring, including support for AAA and SNMP, is required for these systems.

Effectiveness (Application Acceleration, compression, Auto-Discovery) – Greater then 80% data reduction is desired. Also, HTTP caching, separate from byte level caching is desired. . Data compression is required, normally using both layer 6 and 7 servicing of applications. Different compression algorithms can be used including LZ compression. Data Store or Byte level caching storage capability of 3 Terabytes or higher is required. This allows for a FIFO queue technique for byte cache instances to stay in the optimizer for as long as possible in case that cache instance is referenced again, which would keep it off the Wan circuit. Auto discovery allows the appliances to create optimized connections with other WAN optimizers in a dynamic fashion, removing the need to statically set up the peering between med centers and data center throughout the VA.

EVALUATION FACTORS

- Ease of installation and maintenance is of prime importance in choosing a standard for WAN Optimization. Ease of maintenance is the most important factor as problems can develop with applications and traffic types that may stop users from being able to do their job.
- Visibility of connections statistics and pass through variables can help in the trouble shooting of problems being caused by the WAN optimizers. The manageability of these systems is just as important as the benefits they provide.
- Vendor support needs to be considered as evaluating factor. This can be ascertained by talking to other customers and searching the Internet for testimonial information.
- Though not a requirement, transparency mode is useful when looking at a WAN Optimization standard. This allows the IP addresses of the actual server/client will be preserved instead of the traffic being tunneled using the IP addresses of the Wan optimizers.
- WAN monitoring and reporting as well as QOS schemes can run in the same manner before the installation of WAN Optimizers. Again, this is not required because most optimizers provide a method of doing these things but it should be considered.

IMPLEMENTATION GUIDANCE

Capacity will need to be determined by calculating the required concurrent number of workstation connections to the Data Center that needs acceleration. Without Exchange, recommended estimations have been identified 5 to 10 connections per workstation plus 15% growth as a guide to determine necessary capacity at the Data Center.

Many factors need to be considered while deploying and maintaining WAN optimizers. Many applications evolve or are upgraded on the client and server systems and this can have a detrimental effect on the method and effectiveness of the way the WAN optimizer operates. For instance, when MS Office was upgraded to 2007, encryption was turned on in all client systems in regards to their connections to the Exchange server. Most optimizers cannot effectively accelerate or compress encrypted or previously compressed data going across the wire. The staff that is responsible for the operations of the Optimizers must participate in all groups involved in changing profiles and applications on servers and clients. SMB signing and SMBv2 is another example of data types

that may cause issues. It will be important to use WAN optimizers that can handle these kinds of security requirements and changes.

4 TAXONOMY OF STANDARDS

ID	*Primary Attribute*	*Secondary Attribute*
1	Platform Chassis	Type (Modular vs. Static)
		System Throughput
		Packet Processor Redundancy Support
		Control Plane Redundancy Support
		Cooling Redundancy Support
		Power Supply Redundancy Support
		Front-Back Airflow Support
		Online Insertion/Removable Hot-Pluggable Support
2	Platform Packet Processor	Type (Upgradable)
		Packet processor Redundancy
		Layer 3 Routing Throughput (pps)
		Online Insertion/Removable Hot-Pluggable Support
		Memory (DRAM/Flash)
3	Platform Interface Cards	Interface Speed
		Interface Media Flexibility Support
		Queuing Properties
		Online Insertion/Removable Hot-Pluggable Support
4	Platform Operating System	Type (Modular)
		Features Supported
		Routing Protocols
		Quality of Service
		Protocols Supported
		Network Management
5	Platform Supportability	Technical Support

		Parts replacement
6	Platform Maturity	Operating System Maturity
		Hardware Maturity
		Quality Assurance Certification
7	WAN	Latency
		Transport Method
		Reliability/SLA/Packet Loss
		Path Diversity (Includes Local Loop)
		Carrier Diversity
		Capacity
		Quality of Service
		Networx Carriers
		Traffic Analysis / Probes
9	Network Management	Out of Band Management
		Capacity Planning
		Network Management Protocols
		AAA
		Throughput
10	WAN Encryption	FIPS 140-2 Certification
		Throughput
		Hardware vs Software
		Latency
		Performed using Encapsulation(Tunneling) vs. Payload
		Supported Connection Count
		Cryptography
		Jumbo Frame Support
		Interface Type
		Bypass Capability
11	WAN Acceleration	Capacity
		Interface Type

		Implementation (inline vs. redirection)
		Redundancy
		Traffic Types Supported
		Centralized Management and Reporting
		Connection Management / Visibility
		Effectiveness (Application Acceleration, compression, Auto-Discovery)

APPENDIX A – DEFINITIONS

Click here to enter definitions.

APPENDIX B – REFERENCES

Click here to enter a list of references.

APPENDIX C – ACRONYMS

Refer to the VA Acronym Lookup Web page for a list of VA specific acronyms.

EIE VA OI&T Enterprise Infrastructure Engineering

Click here to enter additional acronyms.

APPENDIX D – CONTRIBUTORS

The following subject matter experts have contributed to the development of this document as indicated

Name	Organization	Role
Adames, Juan	Region 3	
Ashe, David	Region 1	
Benson, Gary	Region 1	
Branch, Gary	Region 4	
Carpenter, Marc	EIE	
Cunagin, Mike	Region 1	
Dahl, Tim	EIE	
Delong, Andrew	EIE	
Dugan, Mike	Region 2	
Finn, Mickey	EIE	
Haislip, Hal	Region 2	
Hina, John	FOD	
Julian, Michael	EIE	
Mehl, John	FOD	
Kinn, Eric	Region 4	
Moser, Robert	Region 1	
O'Brien, Casey	CDCO	
Paul, Tony	Region 5	
Trey, Marty	EIE	

APPENDIX E – MPLS SLA

Service	Key Performance Indicator (KPI)	Service Level	Performance Standards	Acceptable Quality Level	Penalty (Incident -Based Credits - are based on a single occurrence of service delivery)
Network-Based IP VPN	Availability (VPN)	Routine	99.90%	≥ 99.9%	No usage charge should apply during the period of the outage. The MRC for a service that was interrupted by an outage shall be prorated if the outage duration exceeded 12 minutes and was less than the duration required to qualify for a Time to Restore credit. This credit does not apply if the TTR credit is applicable. The amount of credit due for eligible service outages shall be calculated as follows: Credit =(MRC for the service that experienced the outage x (.025) x (duration of the outage in hours and tenths of an hour minus 0.2 hours (12 minutes)))
		Critical	99.99%	≥ 99.99%	
	Latency (CONUS) (Note 1)	Routine	70 ms	≤ 70 ms	Best Effort
	Latency (OCONUS) (Note 2)	Routine	150 ms	≤ 150 ms	Best Effort
	Time to Restore	With Dispatch (Note 4)	8 hours	≤ 8 hours	Customer is entitled to 50% of the MRC for the service, unless failure was due to documented delays caused by customer
		Without Dispatch (Note 3)	4 hours	≤ 4 hours	
	Provisioning	Routine	45 days		Credit is equal to 50% of the Non-Recurring Charge(s) (NRC(s)) or 50% of the MRC(s) for the entire order, whichever is greater, unless the failure to meet this performance objective was due to documented delays by the customer
		Critical	23 day		
	Disconnect	All	30 days		Best Effort

Notes:
1. Latency value is the average round trip transmission between Agency premise routers for an IP VPN with all of its CONUS sites. Latency metric does not apply for DSL, Cable High Speed, Wireless, and Satellite access methods. Relevant standards are RFC 1242 and RFC 2285. The contractor may propose to the Government more cost effective test and

measurement technique alternatives that meet or exceed the requirements in RFC 1242 and RFC 2285.

2. Latency value is the average round trip transmission between Agency premise routers for an IP VPN with its CONUS and OCONUS sites. Latency metric does not apply for DSL, Cable High Speed, Wireless, and Satellite access methods. Relevant standards are RFC 1242 and RFC 2285. The contractor may propose to the Government more cost effective
test and measurement technique alternatives that meet or exceed the requirements in RFC 1242 and RFC 2285.

3. VPN availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the VPN is operationally available to the Agency. Availability is computed by the standard formula:

$$Av(VPN) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INFORMATION AND TECHNOLOGY

ENTERPRISE INFRASTRUCTURE ENGINEERING

VA Enterprise IT Infrastructure Standard

Server Platform

PRODUCTION V1.0

November 18, 2009

TABLE OF CONTENTS

1 Introduction 1

1.1 Purpose 1

1.2 Objectives 1

1.3 Scope 1

1.4 standards classifications 3

2 Standards 4

2.1 Class C SERVER 5

2.2 class B server 10

2.3 class A server 15

2.4 class E server 19

3 Supporting Details for Standards 24

3.1 LIGHT WORKLOAD **(CLASS C)** 24

3.1.1 Processor 24

3.1.2 Performance 25

3.1.3 Memory 25

3.1.4 Internal Storage 26

3.1.5 External storage interface 28

3.1.6 Server communications Interface 29

3.1.7 Removable Media Device 31

3.1.8 Power 32

3.1.9 Cooling Fan 33

3.1.10 Out of Band Management 34

3.1.11 Server Hardware Vendor Support 34

3.1.12 Hardware Management Software 35

3.1.13 Rack Infrastructure compatibility 36
3.1.14 Operating System 37
3.1.15 Platform Software / License 38
3.1.16 Datacenter Management 39
3.2 TYPICAL WORKLOAD **(CLASS B)** 40
3.2.1 Processor 40
3.2.2 Performance 41
3.2.3 Memory 42
3.2.4 Internal Storage 43
3.2.5 External storage interface 45
3.2.6 Server communications Interface 46
3.2.7 Removable Media Device 47
3.2.8 Power 48
3.2.9 Cooling Fan 49
3.2.10 Out of Band Management 50
3.2.11 Server Hardware Vendor Support 50
3.2.12 Hardware Management Software 51
3.2.13 Rack Infrastructure compatibility 52
3.2.14 Operating System 53
3.2.15 Platform Software / License 54
3.2.16 Datacenter Management 55
3.3 HEAVY WORKLOAD (**CLASS A**) 56
3.3.1 Processor 56
3.3.2 Performance 57
3.3.3 Memory 58
3.3.4 Internal Storage 59
3.3.5 External storage interface 61

3.3.6 Server communications Interface 62
3.3.7 Removable Media Device 63
3.3.8 Power 64
3.3.9 Cooling Fan 65
3.3.10 Out of Band Management 66
3.3.11 Server Hardware Vendor Support 66
3.3.12 Hardware Management Software 67
3.3.13 Rack Infrastructure compatibility 68
3.3.14 Operating System 69
3.3.15 Platform Software / License 70
3.3.16 Datacenter Management 71
3.4 Vista back-end (BE) (**CLASS E**) 72
3.4.1 Processor 73
3.4.2 Performance 74
3.4.3 Memory 75
3.4.4 Internal Storage 75
3.4.5 External storage interface 77
3.4.6 Server communications Interface 78
3.4.7 Removable Media Device 80
3.4.8 Power 80
3.4.9 Cooling Fan 81
3.4.10 Out of Band Management 83
3.4.11 Server Hardware Vendor Support 84
3.4.12 Hardware Management Software 85
3.4.13 Rack Infrastructure compatibility 86
3.4.14 Operating System 86
3.4.15 Platform Software / License 87

3.4.16 Datacenter Management 89

4 Taxonomy of Standards 89

Appendix A – Definitions 93

Appendix B – References 93

Appendix C – Acronyms 94

Appendix D – Contributors 94

Appendix F – SERVER CLASSES 96

Appendix G – Disk subsystem PERFORMANCE test 97

1 INTRODUCTION

1.1 PURPOSE

A standard is a set of rules or requirements that are determined by a consensus opinion of subject matter experts and prescribe criteria for a product, process, test or procedure. The general benefits of a standard are quality, interchangeability of parts or systems, and consistency. Information Technology (IT) standards are based on business needs provided through or supported by IT Services. IT Services are designed to support business processes and are constructed from software, hardware and infrastructure components. Establishing and enforcing standards for the selection and configuration of these supporting components improves the maintainability, reliability and availability of IT Services within projected economic constraints in alignment with business needs.

This standards document lists the acceptable and recommended specifications for Server Platforms. Sections include standard specifications for subject components, decisions supporting the standard specifications, guidelines or recommendations for implementing the standard specifications, and supplemental factors to consider for when evaluating subject components. Other supplementary documents will provide guidance on procuring components that meet the standard specifications, guidance on integrating them with existing components, and explanation of how the subject components fit into the VA Architecture.

1.2 OBJECTIVES

This standard provides acceptable and recommended specifications to support:

- Solution Evaluation
- Requirement Evaluation
- Solution Design
- Solution Procurement and Bid Evaluation
- Evaluation of Architectural Specifications
- Click here to enter Specific Objectives

1.3 SCOPE

This standard applies to:

- Specifications will include all attributes necessary to specify x86 class servers:
    - Server Hardware
    - Operating System
    - Supporting Equipment Rack Infrastructure

- All solutions that seek inclusion to the VA infrastructure undergo a technical analysis review (TAR). The TAR process is designed to ensure that all solutions meet the standards defined herein. A waiver can be granted if the solution can not meet the standards. Requests for waivers must go through the TAR process.
- To understand the TAR/TAS process, please refer to the following publications:
    - Anatomy of TAR Email Request.pdf
    - TAR-TAS Process-Steps.pdf
    - TAR Request Form - Project Name.docx

1.4 STANDARDS CLASSIFICATIONS

The server standards are divided into classes which encompass the needs of most current and future systems. The goal of the server classes is to simplify the platform selection process and to gain efficiencies in management of the platform. Having fewer standardized server platforms enables more efficient provisioning or re-provisioning of systems, the ability to have a test lab that accurately represents production options, and the ability to pre-buy systems enabling more rapid response to customer requests for new or increased capacity.

The server classes are derived through the analysis of server functions and workloads. Server functions are organized into four categories: content delivery, application server, transactional, and virtualization. To each of these categories is assigned three workloads: light, typical, and heavy. An evaluation of server function and workload exposes commonality among server requirements which leads to a concise set of server classes or sets of standards that can be used to accommodate most solution designs.

General Description of Server Functions:

Content Delivery – Examples: web server, FTP, file server, Active Directory / Domain Controller, SharePoint web portal, management server, print servers, DHCP servers

Application Server – Examples: WebLogic server, VistA front-end server, Terminal Server, SharePoint application tier server

Transactional – Examples: Database server, SharePoint MOSS server, data backup server

Virtualized Host – Examples: virtualization farm, virtualized content, application, or transactional servers

General Description of Server Classes:

Class A, the largest of the classes, targets transactional servers and virtualized host platforms with heavy workloads. Class B, having less performance and I/O capabilities than Class A, targets transactional servers with light to typical workloads and application and content delivery servers with heavy workloads. Class C is designed for content delivery servers with light to typical workloads. It should be noted that Class C servers still maintain significant performance characteristics and offer a smaller form factor then do class A and B servers. The class D specification has been set aside for a future standard which addresses cloud computing designs. Class E servers are transactional servers based on the Itanium processor and are used exclusively for VistA back-end (VistA BE) database servers. Class E servers are an exception to typical transactional servers defined by classes A and B.

Class A – VM hosts, heavy workload transactional

Class B –Heavy workload application servers, Heavy workload content delivery, light and typical workload transactional

Class C – Light and typical workload application servers, Light and typical workload content delivery, web servers

Class D – This class is based on cloud computing environments and has yet to be defined.

Class E – Typical to heavy workload Itanium based servers used exclusively for VistA BE designs.

The advantages and disadvantages of consolidating server types into fewer sets of defined categories, each with the highest "minimum" configuration required to serve the multiple roles, are:

Advantages:

- Allows easy structure of IDIQ contract
- Quicker to document
- Cost of buying extra memory, interfaces, is relatively small compared to overall cost and is less than trying to add those resources later through a server upgrade
- Simpler document to use for the audience/consumer when architecting or purchasing solutions
- Easier to re-provision for different workload or to modify workload on servers
- Easier to build/re-build and model test environments with a smaller variation of server types, and less chance of using "approximations" of server types in the test environments which can lead to higher quality of test results
- Creates a more converged standardization of servers in the data center for easier management and operations
- Easier to "pre-buy" the servers to set up a "utility" type of data center resource

Disadvantages:

- Less cost-efficient for initial (capital) acquisition costs
- Lower efficiency in operational utilization of resources, leading to more power consumption
- Potential for over-consumption of rack space (and subsequently floor space, more power circuits, more network infrastructure capacity assigned to racks)

How to Apply these Standards:

Server classes appear in this document in the following order: C, B, A, E. With the exception of the Class E server, the server classes are listed in order of workload capability from the lightest to the heaviest. The requirements of the Class E server represent an exception to the core standards set forth in this document and have been placed at the end.

Starting with the Class C server, each class adds to the previous class' characteristics in a way that increases its workload capability. The Class C server represents the least common denominator of all server classes – possessing the characteristics that fulfill many general purpose computing needs. These characteristics are refined as the workload requirements of the server increase, so that the Class B server has all of the Class C characteristics plus additional components (memory, processing capacity, etc.) to support its intended use. The Class A server, the largest server class, has all the Class B characteristics plus the additional components (again, largely memory, processing capacity, network connections, etc.) for its workload requirements.

As a general rule, servers should be procured to meet the requirements of their proposed workload. When applying these standards in a procurement process, the reader should first identify the function the server will perform and the workload the function will place on the server. Appendix F provides a list of common server functions and workloads and associates them with recommended server classes

It should be noted that for all classes, **the standards are the baseline specifications** and add-on requirements/enhancements can be used for system design and/or procurement – ex: additional NICs or RAM for certain workloads.

*** See Appendix F for table of server classes.**

2 STANDARDS

2.1 CLASS C SERVER

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
1	Processor	Type	x86_64 (e.g., Intel Xeon, AMD Opteron)
		Socket Count	Minimum required to meet Performance Benchmark standard
		Core Count	Amount required to meet Performance Benchmark standard
		Cache	Minimum total 2MB L2 Cache on chip
		Virtualization Aware	Not Required
2	Performance	Performance Benchmark	SPEC CPU2006 Integer Rate Base value >= 175
3	Memory	Type	Compatible with CPU with full error correction capability including ECC; all memory modules must be of the same type and size.
		Total Memory	Minimum 16GB usable
		Speed	Minimum – match operational CPU and bus speed required to meet the Performance Benchmark requirement
4	Internal Storage	Type	SAS RAID controller supporting SAS or SATA drives and RAID/hot-spare features specified for this server
		Quantity of Drives	Minimum three
		RAID Configuration	Minimally require 2 disks in RAID1, plus 1 as hot spare, for page/swap, dump file, and options operating system functional role. Additional local storage needs (e.g., "temp file" storage for a transaction server or standalone storage configurations) are satisfied by additional drives in RAID level 1, 5, or 10 configuration, with a hot spare which can be shared with the page/swap disk's hot spare.
		Drive Speed	Minimum 10K RPM
		Drive Capacity	Minimum 70GB usable storage capacity
		Disk Subsystem Performance	The disk raid group must meet or exceed the performance levels specified for tests "Transaction Rate" and "Throughput Rate" Validation will be incorporated in

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
			user acceptance phase.
		Controller Cache	Minimum 256MB
		Quantity of Controllers	Minimum of one
5	External Storage Interface	Type	Fiber-channel with duplex LC connectors, CPU bus type is PCI-E Or Ethernet matching connector type of storage-dedicated network in data center
		Port Count	Minimum of two
		Bandwidth	Minimum 4Gbps for optical or 1Gbps for copper; must meet or exceed SAN fabric requirements
		Compatibility	Support storage arrays at deployment location; supported by operating system and multipath drivers specified for this server
		SAN Boot Capability	BIOS support for SAN boot
		Blade Chassis Component (if applicable)	Dual embedded switches
		Hardware Redundancy	Supports connecting redundant ports configured to separate switches on the SAN; minimum redundant ports. Support for link aggregation.
6	Server Communications Interface	Type	Ethernet matching connector type for network in data center
		Port Count	Minimum of 2 ports; at least 2 more if private cluster interconnect is required
		Bandwidth	Minimum 1Gbps
		Hardware Redundancy	Supports connecting redundant ports configured to separate switches on the LAN; supports redundant ports (may include embedded ports) for each interface function (e.g., public network function and cluster interconnect function)
		Blade Chassis Component (if applicable)	Dual embedded switches

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
7	Removable Media Device	Optical Drive	(optional) CD/DVD drive – minimum 24x speed
		USB	USB v2.0 port
8	Power	Redundancy	N+1 redundancy on power supply
		Voltage	115-208V input voltage on power supplies
		Cord Type	IEC
		Power Efficiency	Until such time that there are Energy Star ratings available to most server classes, power efficiency should be consistent with industry trends.
		Power Consumption Documentation	Vendor-supplied data for power consumption of specified configuration at 100% load, “typical” active usage, and at idle.
9	Cooling Fan	Redundancy	Minimum N+1 redundancy
10	Out of Band Management	Type	Remote command-line and console-level access utilizing dedicated network interface
		Security	Secure IP-based remote management that complies with all VA security requirements
		Remote Power Control	Ability to remotely power on/off/reset server
11	Server Hardware Vendor Support	Type	Match service level requirement for hosted applications; mission-critical level support shall include 24x7 coverage 365 days/year, less than 1 hour initial engineer-level response time, 4-hour on-site response time for emergency dispatches, and 8-hour time-to-repair
		Term Length	Minimum of three years with two additional option years
		Keep Your Hard Drive	All storage drives are kept by VA in the event of warranty/service replacement
12	Hardware Management Software	Type	Agent or agent-less server management tool accessible through SNMP
		Automated Notification	Hardware events including exceptions, diagnostics, and failures, shall be exposed through SNMP with documented MIBs
		Shared Repository	Allows uploading all information collected by the tool into shared repository using ODBC or JBDC in a manner

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
			that preserves data fields for the diagnostic information (e.g., date/time, error code, module, description, system identification, status, system configuration) Refer to Datacenter Standards, section _____(name, no numbers)
		Support Level	Support level of management software must match support level of server hardware
13	Rack Infrastructure Compatibility	Rack Unit Measurement	1U or 2U for rack-mount servers; blade implementations will be evaluated on an individual basis.
		Rail Type	Tool-less square-hole sliding
		Cable Management	Side-reversible for non-blade solutions
14	Operating System	Type	Linux preferred based on federal requirement to utilize open source operating systems, Windows acceptable, all must VA approved operating systems and compatible with hardware.
		Version	Current target version of Linux or Windows per VA TRM
		Vendor-Installed	Depends on data center policy; default is factory-installed with default settings and most recent patch level
		Support Level / Term	Must match hardware service level; term is three years with two option years unless VA has a standing enterprise software support agreement pertinent OS.
15	Platform Software / License	Multipath	Provides automated load balancing (all paths active) and fail-over; compatible with target storage array
		Data Backup	(optional) Matches requirements of the deployment location data center and SAN backup solution
		Monitoring Tool	Matches requirements of the deployment location data center
		Layered Framework	Defined by the application owner – meet license requirements for this server
		Server Management Tools	Matches requirements of the deployment location data center
		Availability / Recovery Tools	Matches the requirements for Persistent Computing standards applied to the hosted applications/services
		Security Tools	Follows Office of Information and Technology standards

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
			including compliance with FIPS, FISMA, and VA Directives.
		Virtual Management Software	Not Required
16	Datacenter Management	Remote Keyboard/Video/Mouse Control	Ability to remotely connect to the server's external keyboard, video, and mouse ports through a networked KVM switch.
		Remote Power Disconnect	Ability to remotely disconnect/reconnect server to power source

2.2 CLASS B SERVER

[Populate this table from the taxonomy in section 4 and enter specifications as necessary. Replace this paragraph with a brief description of this specification set.

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
1	Processor	Type	x86_64 (e.g., Intel Xeon, AMD Opteron)
		Socket Count	Minimum required to meet Performance Benchmark standard
		Core Count	Amount required to meet Performance Benchmark standard
		Cache	Minimum total 2MB L2 Cache on chip (6MB or greater L3 Cache required for transactional servers)
		Virtualization Aware	Not Required
2	Performance	Performance Benchmark	SPEC CPU2006 Integer Rate Base value >= 200
3	Memory	Type	Compatible with CPU with full error correction capability including ECC; all memory modules must be of the same type and size.
		Total Memory	Minimum 48GB usable
		Speed	Minimum – match operational CPU and bus speed required to meet the Performance Benchmark requirement
4	Internal Storage	Type	SAS RAID controller supporting SAS drives and RAID/hot-spare features specified for this server
		Quantity of Drives	Minimum three
		RAID Configuration	Minimally require 2 disks in RAID1, plus 1 as hot spare, for page/swap, dump file, and options operating system functional role. Additional local storage needs (e.g., “temp file” storage for a transaction server or standalone storage configurations) are satisfied by additional drives in RAID level 1, 5, or 10 configuration, with a hot spare which can be shared with the page/swap disk’s hot spare.
		Drive Speed	Minimum 10K RPM
		Drive Capacity	Minimum 300GB usable storage capacity

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
		Disk Subsystem Performance	The disk raid group must meet or exceed the performance levels specified for tests “Transaction Rate” and “Throughput Rate” Validation will be incorporated in user acceptance phase.
		Controller Cache	Minimum 256MB
		Quantity of Controllers	Minimum of one
5	External Storage Interface	Type	Fiber-channel with duplex LC connectors, CPU bus type is PCI-E Or Ethernet matching connector type of storage-dedicated network in data center
		Port Count	Minimum of two
		Bandwidth	Minimum 4Gbps for optical or 1Gbps for copper; must meet or exceed SAN fabric requirements
		Compatibility	Support storage arrays at deployment location; supported by operating system and multipath drivers specified for this server
		SAN Boot Capability	BIOS support for SAN boot
		Blade Chassis Component (if applicable)	Dual embedded switches
		Hardware Redundancy	Supports connecting redundant ports configured to separate switches on the SAN. Minimum two adapters with minimum one port per adapter. Support for link aggregation.
6	Server Communications Interface	Type	Ethernet matching connector type for network in data center
		Port Count	Minimum of 2 ports; at least 2 more if private cluster interconnect is required
		Bandwidth	Minimum 1Gbps
		Hardware Redundancy	Supports connecting redundant ports configured to separate switches on the LAN; supports redundant ports (may include embedded ports) for each interface function (e.g., public network function and cluster

ID	Primary Attribute	Secondary Attribute	Specification
			interconnect function)
		Blade Chassis Component (if applicable)	Dual embedded switches
7	Removable Media Device	Optical Drive	(optional) CD/DVD drive – minimum 24x speed
		USB	USB v2.0 port
8	Power	Redundancy	N+1 redundancy on power supply
		Voltage	115-208V input voltage on power supplies
		Cord Type	IEC
		Power Efficiency	Until such time that there are Energy Star ratings available to most server classes, power efficiency should be consistent with industry trends.
		Power Consumption Documentation	Vendor-supplied data for power consumption of specified configuration at 100% load, “typical” active usage, and at idle.
9	Cooling Fan	Redundancy	Minimum N+1 redundancy
10	Out of Band Management	Type	Remote command-line and console-level access utilizing dedicated network interface
		Security	Secure IP-based remote management that complies with all VA security requirements
		Remote Power Control	Ability to remotely power on/off/reset server
11	Server Hardware Vendor Support	Type	Match service level requirement for hosted applications; mission-critical level support shall include 24x7 coverage 365 days/year, less than 1 hour initial engineer-level response time, 4-hour on-site response time for emergency dispatches, and 8-hour time-to-repair
		Term Length	Minimum of three years with two additional option years
		Keep Your Hard Drive	All storage drives are kept by VA in the event of warranty/service replacement
12	Hardware Management Software	Type	Agent or agent-less server management tool accessible through SNMP
		Automated Notification	Hardware events including exceptions, diagnostics, and failures, shall be exposed through SNMP with

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
			documented MIBs
		Shared Repository	Allows uploading all information collected by the tool into shared repository using ODBC or JBDC in a manner that preserves data fields for the diagnostic information (e.g., date/time, error code, module, description, system identification, status, system configuration)
		Support Level	Support level of management software must match support level of server hardware
13	Rack Infrastructure Compatibility	Rack Unit Measurement	1U or 2U for rack-mount servers; blade implementations will be evaluated on an individual basis.
		Rail Type	Tool-less square-hole sliding
		Cable Management	Side-reversible for non-blade solutions
14	Operating System	Type	Linux preferred based on federal requirement to utilize open source operating systems, Windows acceptable, all must VA approved operating systems and compatible with hardware.
		Version	Current target version of Linux or Windows per VA TRM
		Vendor-Installed	Depends on data center policy; default is factory-installed with default settings and most recent patch level
		Support Level / Term	Must match hardware service level; term is three years with two option years unless VA has a standing enterprise software support agreement pertinent OS.
15	Platform Software / License	Multipath	Provides automated load balancing (all paths active) and fail-over; compatible with target storage array
		Data Backup	(optional) Matches requirements of the deployment location data center and SAN backup solution
		Monitoring Tool	Matches requirements of the deployment location data center
		Layered Framework	Defined by the application owner – meet license requirements for this server
		Server Management Tools	Matches requirements of the deployment location data center
		Availability / Recovery Tools	Matches the requirements for Persistent Computing

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
			standards applied to the hosted applications/services
		Security Tools	Follows Office of Information and Technology standards including compliance with FIPS, FISMA, and VA Directives.
		Virtual Management Software	Not Required
16	Datacenter Management	Remote Keyboard/Video/Mouse Control	Ability to remotely connect to the server's external keyboard, video, and mouse ports through a networked KVM switch.
		Remote Power Disconnect	Ability to remotely disconnect/reconnect server to power source

2.3 CLASS A SERVER

[Populate this table from the taxonomy in section 4 and enter specifications as necessary. Replace this paragraph with a brief description of this specification set.

ID	***Primary Attribute***	***Secondary Attribute***	***Specification***
1	Processor	Type	x86_64 (e.g., Intel Xeon, AMD Opteron)
		Socket Count	Minimum required to meet Performance Benchmark standard
		Core Count	Amount required to meet Performance Benchmark standard
		Cache	Minimum total 2MB L2 Cache on chip (6MB or greater L3 Cache required for transactional servers)
		Virtualization Aware	Required to facilitate live migration
2	Performance	Performance Benchmark	SPEC CPU2006 Integer Rate Base value >= 250
3	Memory	Type	Compatible with CPU with full error correction capability including ECC; all memory modules must be of the same type and size.
		Total Memory	Minimum 128GB usable
		Speed	Minimum - match operational CPU and bus speed required to meet the Performance Benchmark requirement
4	Internal Storage	Type	SAS RAID controller supporting SAS drives and RAID/hot-spare features specified for this server
		Quantity of Drives	Minimum three
		RAID Configuration	Minimally require 2 disks in RAID1, plus 1 as hot spare, for page/swap, dump file, and options operating system functional role. Additional local storage needs (e.g., “temp file” storage for a transaction server or standalone storage configurations) are satisfied by additional drives in RAID level 1, 5, or 10 configuration, with a hot spare which can be shared with the page/swap disk’s hot spare. When this class of server is configured as a transaction

ID	Primary Attribute	Secondary Attribute	Specification
			server, a separate RAID controller or second channel on the same controller is required for the “temp file” RAID group
		Drive Speed	Minimum 10K RPM
		Drive Capacity	Minimum 450GB usable storage capacity
		Disk Subsystem Performance	The disk raid group must meet or exceed the performance levels specified for tests “Transaction Rate” and “Throughput Rate” Validation will be incorporated in user acceptance phase.
		Controller Cache	Minimum 256MB
		Quantity of Controllers	Minimum of one
5	External Storage Interface	Type	Fiber-channel with duplex LC connectors, CPU bus type is PCI-E Or Ethernet matching connector type of storage-dedicated network in data center
		Port Count	Minimum of 2 independent cards with a minimum of 2 ports each
		Bandwidth	Minimum 4Gbps for optical or 1Gbps for copper; must meet or exceed SAN fabric requirements
		Compatibility	Support storage arrays at deployment location; supported by operating system and multipath drivers specified for this server
		SAN Boot Capability	BIOS support for SAN boot
		Blade Chassis Component (if applicable)	Dual embedded switches
		Hardware Redundancy	Supports connecting redundant ports configured to separate switches on the SAN. Minimum two adapters with minimum one port per adapter. Support for link aggregation.
6	Server Communications Interface	Type	Ethernet matching connector type for network in data center
		Port Count	Minimum of 6 ports; more may be necessary depending

ID	Primary Attribute	Secondary Attribute	Specification
			on virtual infrastructure requirements
		Bandwidth	Minimum 1Gbps
		Hardware Redundancy	Supports connecting redundant ports configured to separate switches on the LAN; supports physically independent redundant ports including embedded ports for each interface function (e.g., public network function and cluster interconnect function)
		Blade Chassis Component (if applicable)	Dual embedded switches
7	Removable Media Device	Optical Drive	(optional) CD/DVD drive – minimum 24x speed
		USB	USB v2.0 port
8	Power	Redundancy	N+1 redundancy on power supply
		Voltage	208V input voltage on power supply
		Cord Type	IEC
		Power Efficiency	Until such time that there are Energy Star ratings available to most server classes, power efficiency should be consistent with industry trends.
		Power Consumption Documentation	Vendor-supplied data for power consumption of specified configuration at 100% load, “typical” active usage, and at idle.
9	Cooling Fan	Redundancy	Minimum N+1 redundancy
10	Out of Band Management	Type	Remote command-line and console-level access utilizing dedicated network interface
		Security	Secure IP-based remote management that complies with all VA security requirements
		Remote Power Control	Ability to remotely power on/off/reset server
11	Server Hardware Vendor Support	Type	Match service level requirement for hosted applications; mission-critical level support shall include 24x7 coverage 365 days/year, less than 1 hour initial engineer-level response time, 4-hour on-site response time for emergency dispatches, and 8-hour time-to-repair
		Term Length	Minimum of three years with two additional option years

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
		Keep Your Hard Drive	All storage drives are kept by VA in the event of warranty/service replacement
12	Hardware Management Software	Type	Agent or agent-less server management tool accessible through SNMP
		Automated Notification	Hardware events including exceptions, diagnostics, and failures, shall be exposed through SNMP with documented MIBs
		Shared Repository	Allows uploading all information collected by the tool into shared repository using ODBC or JBDC in a manner that preserves data fields for the diagnostic information (e.g., date/time, error code, module, description, system identification, status, system configuration)
		Support Level	Support level of management software must match support level of server hardware
13	Rack Infrastructure Compatibility	Rack Unit Measurement	Up to 4U for rack-mount servers; blade implementations will be evaluated on an individual basis.
		Rail Type	Tool-less square-hole sliding
		Cable Management	Side-reversible for non-blade solutions
14	Operating System	Type	Linux preferred based on federal requirement to utilize open source operating systems, Windows acceptable, all must VA approved operating systems and compatible with hardware.
		Version	Current target version of Linux or Windows per VA TRM
		Vendor-Installed	Depends on data center policy; default is factory-installed with default settings and most recent patch level
		Support Level / Term	Must match hardware service level; term is three years with two option years unless VA has a standing enterprise software support agreement pertinent OS.
15	Platform Software / License	Multipath	Provides automated load balancing (all paths active) and fail-over; compatible with target storage array
		Data Backup	(optional) Matches requirements of the deployment location data center and SAN backup solution
		Monitoring Tool	Matches requirements of the deployment location data center

ID	Primary Attribute	Secondary Attribute	Specification
		Layered Framework	Defined by the application owner – meet license requirements for this server
		Server Management Tools	Matches requirements of the deployment location data center
		Availability / Recovery Tools	Matches the requirements for Persistent Computing standards applied to the hosted applications/services
		Security Tools	Follows Office of Information and Technology standards including compliance with FIPS, FISMA, and VA Directives.
		Virtual Management Software	For virtual environments, an Enterprise management tool is required
16	Datacenter Management	Remote Keyboard/Video/Mouse Control	Ability to remotely connect to the server's external keyboard, video, and mouse ports through a networked KVM switch.
		Remote Power Disconnect	Ability to remotely disconnect/reconnect server to power source

2.4 CLASS E SERVER

[Populate this table from the taxonomy in section 4 and enter specifications as necessary. Replace this paragraph with a brief description of this specification set.

ID	Primary Attribute	Secondary Attribute	Specification
1	Processor	Type	IA_64 (Itanium)
		Socket Count	Minimum required to meet Performance Benchmark standard
		Core Count	Amount required to meet Performance Benchmark standard
		Cache	Minimum required to meet Performance Benchmark standard
		Virtualization Aware	Not Required

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
2	Performance	Performance Benchmark	SPEC CPU2006 Integer Rate Base value >= 90
3	Memory	Type	Compatible with CPU with full error correction capability including ECC
		Total Memory	Minimum 24GB usable
		Speed	Minimum - match operational CPU and bus speed required to meet the Performance Benchmark requirement
4	Internal Storage	Type	SAS
		Quantity of Drives	Minimum one (DOSD – i.e. to host Dump Off System Disk)
		RAID Configuration	Not Required
		Drive Speed	Minimum 10K RPM
		Drive Capacity	Minimum 36GB usable storage capacity
		Disk Subsystem Performance	The disk must meet or exceed the performance levels specified below for tests “Transaction Rate” and “Throughput Rate” Validation will be incorporated in user acceptance phase.
		Controller Cache	Not Required
		Quantity of Controllers	Minimum of one
5	External Storage Interface	Type	Fiber-channel with duplex LC connectors
		Port Count	Minimum of four ports with full port redundancy provided.
		Bandwidth	Minimum 4Gbps; must meet or exceed SAN fabric requirements
		Compatibility	Support storage arrays at deployment location; supported by operating system and multipath drivers specified for this server
		SAN Boot Capability	BIOS support for SAN boot
		Blade Chassis Component (if applicable)	Pass thru connections, for increased bandwidth capabilities

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
		Hardware Redundancy	Supports connecting redundant ports configured to separate switches on the SAN. Minimum redundant ports
6	Server Communications Interface	Type	Ethernet matching connector type for network in data center
		Port Count	Minimum of 6 ports
		Bandwidth	Minimum 1Gbps
		Hardware Redundancy	Supports connecting redundant ports configured to separate switches on the LAN; supports physically independent redundant ports including embedded ports for each interface function (e.g., public network function and cluster interconnect function)
		Blade Chassis Component (if applicable)	Pass Thru connections
7	Removable Media Device	Optical Drive	CD/DVD drive – minimum 24x speed
		USB	Not Required
8	Power	Redundancy	N+1 redundancy on power supply
		Voltage	208V input voltage on power supply
		Cord Type	IEC
		Power Efficiency	Until such time that there are Energy Star ratings available to most server classes, power efficiency should be consistent with industry trends.
		Power Consumption Documentation	Vendor-supplied data for power consumption of specified configuration at 100% load, “typical” active usage, and at idle.
9	Cooling Fan	Redundancy	Minimum N+1 redundancy
10	Out of Band Management	Type	Remote command-line and console-level access utilizing dedicated network interface
		Security	Secure IP-based remote management that complies with all VA security requirements
		Remote Power Control	Ability to remotely power on/off/reset server

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
11	Server Hardware Vendor Support	Type	Match service level requirement for hosted applications; mission-critical level support shall include 24x7 coverage 365 days/year, less than 1 hour initial engineer-level response time, 4-hour on-site response time for emergency dispatches, and 8-hour time-to-repair
		Term Length	Minimum of three years with two additional option years
		Keep Your Hard Drive	All storage drives are kept by VA in the event of warranty/service replacement
12	Hardware Management Software	Type	Agent or agent-less server management tool accessible through SNMP
		Automated Notification	Hardware events including exceptions, diagnostics, and failures, shall be exposed through SNMP with documented MIBs
		Shared Repository	Allows uploading all information collected by the tool into shared repository using ODBC or JBDC in a manner that preserves data fields for the diagnostic information (e.g., date/time, error code, module, description, system identification, status, system configuration)
		Support Level	Support level of management software must match support level of server hardware
13	Rack Infrastructure Compatibility	Rack Unit Measurement	7U or 10U for rack-mount servers; 4-slot blade for blade servers
		Rail Type	Tool-less square-hole sliding
		Cable Management	Side-reversible for non-blade solutions
14	Operating System	Type	OpenVMS, Un-Limited User Licensing, VMS clustering, Host Based Volume Shadowing, TCP/IP Services
		Version	OpenVMS version 8.3 (minimum version support)
		Vendor-Installed	Not Required, but preferred
		Support Level / Term	Must match hardware service level; term is three years with two option years unless VA has a standing enterprise software support agreement pertinent OS.
15	Platform Software / License	Multipath	Provides automated load balancing (all paths active) and fail-over; compatible with target storage array

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
		Data Backup	(optional) Matches requirements of the deployment location data center and SAN backup solution
		Monitoring Tool	Matches requirements of the deployment location data center
		Layered Framework	Support for InterSystems' Caché (minimum version 5.2.3)
		Server Management Tools	Matches requirements of the deployment location data center
		Availability / Recovery Tools	Matches the requirements for Persistent Computing standards applied to the hosted applications/services
		Security Tools	Follows Office of Information and Technology standards including compliance with FIPS, FISMA, and VA Directives.
		Virtual Management Software	Not Required
16	Datacenter Management	Remote Keyboard/Video/Mouse Control	Ability to remotely connect to the server's external keyboard, video, and mouse ports through a networked KVM switch.
		Remote Power Disconnect	Ability to remotely disconnect/reconnect server to power source

3 SUPPORTING DETAILS FOR STANDARDS

3.1 LIGHT WORKLOAD **(CLASS C)**

3.1.1 PROCESSOR

STANDARD

ID	*Secondary Attribute*	*Specification*
1	Type	x86_64 (e.g., Intel Xeon, AMD Opteron)
	Socket Count	Minimum required to meet Performance Benchmark standard
	Core Count	Amount required to meet Performance Benchmark standard
	Cache	Minimum total 2MB L2 Cache on chip
	Virtualization Aware	Not Required

EXPLANATION OF STANDARD

Type – open/industry standard components.

Socket Count – minimize due to licensing costs per socket, have minimum count for performance/capacity.

Core Count – minimum amount expected for performance/capacity level is quad-core, more can be better. However, any amount that meets the Performance Benchmark specification is sufficient.

Cache – minimum expected for class of processor; low-power options might use lower amounts of cache.

EVALUATION FACTORS

- Currency of processor – most recent family and speed of processor is beneficial.
- Higher amounts of cache and cores are beneficial.
- Open processor slots or ability to enable additional processors for future expansion could be beneficial in larger configurations.

IMPLEMENTATION GUIDANCE

It is recommended to have a Socket Count of two in order to minimize licensing costs that are calculated on a per socket basis. Exceptions for higher socket count should have justification documented and should consider both performance and cost.

3.1.2 PERFORMANCE

STANDARD

ID	Secondary Attribute	Specification
2	Performance Benchmark	SPEC CPU2006 Integer Rate Base value >= 175

EXPLANATION OF STANDARD

This SPEC_Int rate is represented by a large number of server platforms. Performance requirement is largely dependent on the application's workload and compute-resource consumption profile. The architecture of this server tier may provide sufficient horizontal scaling to accommodate larger workloads, especially with minimum server counts required for redundancy and limit of single-server impact. This specification is a starting point for a "light duty" small-workload content delivery server environment based upon review of existing tested systems in the VA environment and their capabilities represented with newer server offerings. This specification should be adjusted to meet the known workload of target hosted applications and the target architecture for its server tier.

EVALUATION FACTORS

Higher benchmark rating value is beneficial.

IMPLEMENTATION GUIDANCE

3.1.3 MEMORY

STANDARD

ID	Secondary Attribute	Specification
3	Type	Compatible with CPU with full error correction capability including ECC; all memory modules must be of the same type and size.
	Total Memory	Minimum 16GB usable
	Speed	Minimum – match operational CPU and bus speed required to meet the Performance Benchmark requirement

EXPLANATION OF STANDARD

Type – Memory has to be highly reliable – ECC is the expected feature to allow higher levels of reliability. RDIMM is more expandable/scalable and provides additional reliability features (e.g., more error-checking features) while

consuming more power (about one watt per chip) and costing more. In general, RDIMM is recommended with high memory requirements and higher availability requirements.

Total Memory – Memory requirements depend on application needs. The standard must meet the minimum requirement for memory intensive applications that could be run on this class of server. Using WebLogic as an example, minimum expected is 2GB-4GB per CPU core (as per Java configuration guidelines). With current VA application designs, each JVM requires at least 4GB of memory; more if 64 bit JVMs are used. For a typical dual-socket quad-core server running WebLogic, the minimum expected requirement is therefore 16GB. Usable memory value indicates the possibility of RAID or mirrored memory for additional redundancy. When using memory configurations above the minimum, internal storage capacity must be adjusted to support page/swap and dump requirements. This should be calculated using the formula: (2XRAM=page/swap size) + (1XRAM=DUMP) + (20GB for OS)

Speed – At least one operational speed of the memory must match the highest speed capability of the information bus used to retrieve memory for the CPU in order to maximize the investment into the CPU. Features can allow for step-down of speed correlated with workload consumption (power-saving feature).

EVALUATION FACTORS

- Additional memory is beneficial
- Higher density chips while avoiding a decrease in memory bus speed is preferred.
- Speed of memory takes precedence over density as long as capacity is met

IMPLEMENTATION GUIDANCE

RDIMM is recommended for high memory requirements and higher availability requirements.

3.1.4 INTERNAL STORAGE

STANDARD

ID	*Secondary Attribute*	*Specification*
4	Type	SAS RAID controller supporting SAS or SATA drives and RAID/hot-spare features specified for this server
	Quantity of Drives	Minimum three
	RAID Configuration	Minimally require 2 disks in RAID1, plus 1 as hot spare, for page/swap, dump file, and options operating system functional role. Additional local storage needs (e.g., “temp file” storage for a transaction server or standalone storage configurations) are satisfied by additional drives in RAID level 1, 5, or 10 configuration, with a hot spare which can be shared with the page/swap disk’s hot spare.
	Drive Speed	Minimum 10K RPM
	Drive Capacity	Minimum 70GB usable storage capacity

	Disk Subsystem Performance	The disk raid group must meet or exceed the performance levels specified for tests "Transaction Rate" and "Throughput Rate" Validation will be incorporated in user acceptance phase.
	Controller Cache	Minimum 256MB
	Quantity of Controllers	Minimum of one

EXPLANATION OF STANDARD

Type – SAS or SATA drives may be used. While SAS is preferred, SATA may be used where capacity or cost takes precedence over performance. Solid state drives are beneficial due to power, cooling, performance, and reliability, but are expensive and currently are only used sparingly in external storage systems.

Quantity & RAID Configuration – requires performance for a page/swap disk and dump file, with possible additional uses; ability to continue with a drive failure (e.g., RAID1) and restore to this state with an immediately available drive (hot spare). For high performance functions (including page/swap disk), RAID1 is preferred over parity protection due to overhead of calculating parity. Although additional drives may help spread I/O across more drives for enhanced performance, additional drives also add to the cost, maintenance, and power consumption on the server. Therefore, additional drives should only be considered when they are required for performance or capacity reasons. The optimal configuration uses the fewest quantity of drives to meet the performance and reliability requirements. Additional drives are needed for additional storage needs such as a standalone storage configuration which is provided on a separate disk per industry best practice guidance.

Drive Speed – Minimum RPM for this class of server & storage is 10K.

Drive Capacity – 70GB minimum usable storage capacity is sufficient to support an operating system and/or swap and log files. This amount represents the expected minimum required for page/swap file, dump file, and optional system disk storage needs. When using memory configurations above the minimum, internal storage capacity must be adjusted to support page/swap and dump requirements. This should be calculated using the formula: (2XRAM=page/swap size) + (1XRAM=DUMP) + (20GB for OS)

Disk Subsystem Performance – The disk raid group must meet or exceed the performance levels specified below for tests "Transaction Rate" and "Throughput Rate" as described in APPENDIX G.

- Transaction Rate = 500+ IOPS
- Throughput Rate = 50+ MBPS

Controller Cache – minimum expected value for typical controllers for this class of server.

Quantity of Controllers – limited value to have more than one with only one RAID configuration; might be beneficial for more than two RAID sets if performance requires it; current technology offerings limit the ability to fail services over from one controller to another without manual intervention – future technology offerings such as dual-domain active/active configurations in SAS controllers & drives provide this capability

EVALUATION FACTORS

- Higher storage capacity is beneficial
- Higher RPM is beneficial for drive platters
- The optimal configuration uses the fewest quantity of drives to meet the performance and reliability requirements.
- Solid-state drives would be beneficial
- Higher throughput capability is beneficial
- Higher IOPS capability is beneficial
- More controllers can be beneficial
- More cache is beneficial
- Battery backup of cache is beneficial
- Support for RAID levels 0, 1, 5, 6, 0+1, and/or 1+0 is beneficial
- Separate hot spares for separate RAID groups is beneficial.

IMPLEMENTATION GUIDANCE

- SAS interface type is recommended. Battery backup of cache is recommended.

3.1.5 EXTERNAL STORAGE INTERFACE

STANDARD

ID	***Secondary Attribute***	***Specification***
5	Type	Fiber-channel with duplex LC connectors, CPU bus type is PCI-E Or Ethernet matching connector type of storage-dedicated network in data center. TOE / TCP checksum offload required.
	Port Count	Minimum of two
	Bandwidth	Minimum 4Gbps for optical or 1Gbps for copper; must meet or exceed SAN fabric requirements
	Compatibility	Support storage arrays at deployment location; supported by operating system and multipath drivers specified for this server
	SAN Boot Capability	BIOS support for SAN boot
	Blade Chassis Component (if applicable)	Dual embedded switches

	Hardware Redundancy	Supports connecting redundant ports configured to separate switches on the SAN; minimum redundant ports. Support for link aggregation.

EXPLANATION OF STANDARD

- Type – fiber channel and Ethernet are the vast majority of investment for connections used in storage-dedicated networks in VA data centers, and exceptions should be justified including impact to existing infrastructure investment. Typical Ethernet connector types are RJ-45 for copper and LC for optical. When Ethernet is used, TOE / TCP checksum offload is required. Drivers are more readily available for Windows than Linux servers.
- Port Count – minimum required for port-level redundancy / load-balancing
- Bandwidth – 4Gbps is standard for current investment of optical fabrics in the storage systems and infrastructure in VA data centers and matches the minimum current industry standard; similarly 1Gbps is standard for current investments and minimum current industry practices when using copper-based storage fabrics.
- Compatibility – Support storage subsystems at deployment locations. Check adapter compatibility for storage at deployment location.
- Blade Chassis Component – A primary benefit of blade servers is their ability to reduce datacenter cabling. Dual fiber-channel switches (or Ethernet if applicable) are required. Pass-thru configurations require an exception. Each blade chassis shall have redundant sets of embedded switches to provide independent SAN connections to each blade. Each embedded switch set shall have the ability to configure redundant and/or trunked ISL/uplink ports. Minimum number of uplink ports in chassis is two times the number of embedded switches. Refer to Storage Standards, Section xx.
- Hardware Redundancy – Fail-over and load-balancing are functions of the multipath tool which is covered in section 3.2.16

EVALUATION FACTORS

- Redundancy across physically independent interfaces is beneficial
- Support for 8Gbps optical or 10Gbps copper bandwidth is beneficial

IMPLEMENTATION GUIDANCE

- For a server with high criticality of SAN storage connectivity, redundant adapter cards are recommended.
- Interface for iSCSI can be termed an HBA interface or a NIC interface. Where higher performance is a concern, the HBA interface is recommended.
- Bandwidth spread across multiple ports on independent cards may be required for performance reasons

3.1.6 SERVER COMMUNICATIONS INTERFACE

STANDARD

ID	*Secondary Attribute*	*Specification*

6	Type	Ethernet matching connector type for network in data center
	Port Count	Minimum of 2 ports; at least 2 more if private cluster interconnect is required
	Bandwidth	Minimum 1Gbps
	Hardware Redundancy	Supports connecting redundant ports configured to separate switches on the LAN; supports redundant ports (may include embedded ports) for each interface function (e.g., public network function and cluster interconnect function)
	Blade Chassis Component (if applicable)	Dual embedded switches

EXPLANATION OF STANDARD

Type – Ethernet is the vast majority of investment for connections used in data center networks in VA, and exceptions should be justified including impact to existing infrastructure investment. Typical Ethernet connector types are RJ-45 for copper and LC for optical with a future trend towards copper only.

Port Count – base set of 2 ports are for general "public" Ethernet; other specific interfaces may be required depending on the profile of the workload/application. Cluster interconnects may need 2 or more ports, depending on the amount of cluster traffic (e.g., Oracle clusters send data over the cluster interconnect, simple Microsoft clustering only send "heartbeat" traffic).

Bandwidth – expected standard interface on network switches is 1Gbps. There is a potential for 10Gbps Ethernet.

Hardware Redundancy – embedded ports count as one "card" which is sufficient for this class of server except where additional ports are required. If additional ports are required, all interface uses are spread across two "cards" (including at least one add-on NIC). The goal is physical separation of the chipset/ASIC used on the redundant port, for each function. Support for "simple failover" (with a single IP address) and independent usage (with multiple IP addresses) is required.

Blade Chassis Component – Where applicable, blade-server chassis should be configured with two switches to limit port and cabling needs external to the server, unless there is a specific workload/application requirement for high throughput that requires pass-through capability.

EVALUATION FACTORS

- Additional cards can be beneficial
- Support for TCP Offload Engine is beneficial
- Support for active/active load balancing is beneficial

IMPLEMENTATION GUIDANCE

- One or two additional ports are recommended for network backups if the impact of backup traffic may affect other services on the "public" network. One port is sufficient if only one port is active and uses another port for fail-over.

- TCP Offload Engine (TOE) is preferred for all servers. Drivers are more readily available for Windows than Linux servers.
- If there is a specific workload/application requirement for high throughput that requires pass-through capability on a blade-server chassis, then this option should be configured, but the chassis switch is preferred otherwise.

BANDWIDTH SPREAD ACROSS MULTIPLE PORTS ON INDEPENDENT CARDS MAY BE REQUIRED FOR PERFORMANCE REASONS

3.1.7 REMOVABLE MEDIA DEVICE

STANDARD

ID	*Secondary Attribute*	*Specification*
7	Optical Drive	(optional) CD/DVD drive – minimum 24x speed
	USB	USB v2.0 port

EXPLANATION OF STANDARD

The functional requirement supported by this standard is to provide a media transfer mechanism to upload patch and software/firmware installation, upload diagnostic tools, and (with read/write capability) to download diagnostic information. Manufacturers are going toward a trend of using USB flash drives for sending patch/upgrade/firmware distributions. Therefore, the requirement is to provide both CD/DVD and USB flash drive capabilities. Note that security restrictions or concerns need to be addressed before using removable media.

The optical drive is optional because small form factor (e.g., blade) servers might not allow this type of component. These small form factor servers do, however, have the ability to support USB flash drives.

The type of drive specified is the typical expected minimum specification and type.

EVALUATION FACTORS

- Having an optical drive is beneficial.
- Faster speeds and/or Read-write capability is beneficial (additional security checks may be required for read/write capability).

IMPLEMENTATION GUIDANCE

- Preferred to provide removable media device for patch and software installation options; but small form factor (e.g., blade) servers might use other options.

3.1.8 POWER

STANDARD

ID	Secondary Attribute	Specification
8	Redundancy	N+1 redundancy on power supply
	Voltage	115-208V input voltage on power supplies
	Cord Type	IEC
	Power Efficiency	Until such time that there are Energy Star ratings available to most server classes, power efficiency should be consistent with industry trends.
	Power Consumption Documentation	Vendor-supplied data for power consumption of specified configuration at 100% load, "typical" active usage, and at idle.

EXPLANATION OF STANDARD

Redundancy – server must continue to operate if and when a power supply fails in order to enhance availability.

Voltage and cord type – driven by data center standards, 208V can more efficiently use power from utility

Power Efficiency – Certifications for power efficiency include: 80-plus (Dell & HP certify through them, but IBM does not), and Energy Star (still forming the standard for servers, but blade servers will be separate standard). The EPA establishes Energy Star standards – tier 2 appears to be the four-socket type of server while tier 1 appears to be the dual-socket server types. Some server manufacturers implement power efficiency management features including step-down of power consumption during low resource-consumption states.

Power Consumption Documentation – Preferred documentation is Energy Star data sheet and/or SPECpower_ssj2008 published results.

EVALUATION FACTORS

- Power management/economy and reporting/analysis features are beneficial.
- Lower power consumption rating at 100% utilization per workload capacity (in terms of SPECint_rate value) is beneficial.

IMPLEMENTATION GUIDANCE

- Cord type of IEC-C13 is preferred for most classes of rack-mount servers

3.1.9 COOLING FAN

STANDARD

ID	***Secondary Attribute***	***Specification***
9	Redundancy	Minimum N+1 redundancy

EXPLANATION OF STANDARD

Redundancy – server must continue to operate if and when a fan fails in order to enhance availability.

EVALUATION FACTORS

- Additional fans or separation of fans into multiple cooling zones is beneficial.
- Lower total decibel rating on the fans is beneficial.

IMPLEMENTATION GUIDANCE

3.1.10 OUT OF BAND MANAGEMENT

STANDARD

ID	Secondary Attribute	Specification
10	Type	Remote command-line and console-level access utilizing dedicated network interface
	Security	Secure IP-based remote management that complies with all VA security requirements
	Remote Power Control	Ability to remotely power on/off/reset server

EXPLANATION OF STANDARD

Required dedicated network interface is required outside of the other network interfaces specified in section 3.1.7.

Based on data center environment, operational needs, and minimum requirements that are typically satisfied through a wide variety of servers. Includes access for diagnostic capability.

Remote Power Control – Ability to power on/off/reset through server based management.

EVALUATION FACTORS

- Ability to remotely mount a drive or ISO is beneficial. This can be used for software, firmware and OS updates using remote drive mounting, and it minimizes the need for local optical drive.
- Active Directory integration for authentication is beneficial.
- Role-based access control is beneficial.
- Accounting capability is beneficial.
- Strong password compliance is beneficial.
- Accessibility via web browser is beneficial – should support Microsoft Internet Explorer.
- Support for Secure Shell (SSH) connections is beneficial – should be FIPS 140-2 compliant.
- Ability to remotely identify server with visual indicator (e.g., indicator light) is beneficial.

IMPLEMENTATION GUIDANCE

3.1.11 SERVER HARDWARE VENDOR SUPPORT

STANDARD

ID	Secondary Attribute	Specification

11	Type	Match service level requirement for hosted applications; mission-critical level support shall include 24x7 coverage 365 days/year, less than 1 hour initial engineer-level response time, 4-hour on-site response time for emergency dispatches, and 8-hour time-to-repair
	Term Length	Minimum of three years with two additional option years
	Keep Your Hard Drive	All storage drives are kept by VA in the event of warranty/service replacement

EXPLANATION OF STANDARD

Type – the level of support matches the criticality level of the hosted services. Mission-critical level is defined in this standard, and has been shown to be accommodated by major server vendors. Other levels will have to be defined to match the business expectations of that criticality level. A non-critical example would be 8 business hours/weekday phone coverage with next-day response and repair. Access to original server manufacturer support with the option to escalate to senior technicians at VA discretion is required.

Term – some components might only allow three years of support on an initial contract, but option years must be available to extend that to the expected lifetime of the system which is nominally five years.

Keep Your Hard Drive – This is a security requirement that is now a de-facto standard in VA.

EVALUATION FACTORS

- Lower on-site response time is beneficial.
- Lower initial "engineer level" contact response time is beneficial.
- Lower time-to-repair is beneficial.
- Vendor-supplied components stocked as spares near, or at, facility is beneficial.
- Penalty clauses for vendor not meeting support contract provides benefit.
- Allowance for optional parts-delivery/customer-installation of hot swappable components, memory, and drop-in cards beneficial at the VA's option.
- Access to electronic models of equipment being proposed is beneficial. Because electronic models will be used with CAD and visual design applications for datacenter planning, three dimensional models are preferred.

IMPLEMENTATION GUIDANCE

- It is preferred to have vendor-supplied total system replacements able to ship out to the site within 24 hours via overnight shipment means.

3.1.12 HARDWARE MANAGEMENT SOFTWARE

STANDARD

ID	***Secondary Attribute***	***Specification***

12	Type	Agent or agent-less server management tool accessible through SNMP
	Automated Notification	Hardware events including exceptions, diagnostics, and failures, shall be exposed through SNMP with documented MIBs
	Shared Repository	Allows uploading all information collected by the tool into shared repository using ODBC or JBDC in a manner that preserves data fields for the diagnostic information (e.g., date/time, error code, module, description, system identification, status, system configuration) Refer to Datacenter Standards, Section xx
	Support Level	Support level of management software must match support level of server hardware

EXPLANATION OF STANDARD

The tool should allow management of the hardware through a variety of means that interface with SNMP, and must be fully documented with MIBs for all relevant data (hardware events). Integration with VA's Enterprise Exception Log Service (EELS) is a consideration and is enabled through SNMP interfacing.

Ability to access event logs through database connectivity (JDBC or ODBC) is needed for future Enterprise Management Framework tools.

Service could be provided through BIOS feature, OS-level features, or other layered features, and must provide the MIB documentation for accessing the information.

EVALUATION FACTORS

- Ability to integrate with a variety of industry enterprise-level system management tools is beneficial.
- Inclusion of an enterprise-level component with shared repository and correlation analysis features is beneficial.
- Ability to provide management of agent-less systems is beneficial.

IMPLEMENTATION GUIDANCE

- Support for SNMPv3 is preferred.
- A solution design that provides secure connections outside the physical facility is preferred.
- Automated vendor notification of failure, or pre-failure activity, to initiate vendor remediation is preferred.

3.1.13 RACK INFRASTRUCTURE COMPATIBILITY

STANDARD

ID	***Secondary Attribute***	***Specification***
13	Rack Unit Measurement	1U or 2U for rack-mount servers; blade implementations will be evaluated on an individual basis.

	Rail Type	Tool-less square-hole sliding
	Cable Management	Side-reversible for non-blade solutions

EXPLANATION OF STANDARD

Rack Unit Measurement – For this class of server, occupying 4U (or two blade slots) should not be necessary; 1 slot in a half-height blade chassis is fairly equivalent to a 1U rack-mount and 1 slot in a full-height blade chassis is fairly equivalent to a 2U rack-mount. It is expected that this class of server will be a 2U rack mount or single slot full-height blade server.

Rail Type – server must have rail adapters if needed to fit the generic non-proprietary type of rack specified in this standard.

Rack infrastructure standards must match the data center equipment rack standards.

EVALUATION FACTORS

- Lower occupied rack space (per workload) is beneficial

IMPLEMENTATION GUIDANCE

3.1.14 OPERATING SYSTEM

STANDARD

ID	***Secondary Attribute***	***Specification***
14	Type	Linux preferred based on federal requirement to utilize open source operating systems, Windows acceptable, all must VA approved operating systems and compatible with hardware.
	Version	Current target version of Linux or Windows per VA TRM
	Vendor-Installed	Depends on data center policy; default is factory-installed with default settings and most recent patch level
	Support Level / Term	Must match hardware service level; term is three years with two option years unless VA has a standing enterprise software support agreement pertinent OS.

EXPLANATION OF STANDARD

Type – Linux is preferred as the most “open” type of option, but Windows is also acceptable as an industry-wide supported option. If UNIX is required Solaris is the preferred UNIX product. Solaris is preferred due to the “open” features and high level of government security certification.

Version – Operating system build, distribution, and version must be listed in the VA TRM.

Vendor-Installed – Data center policy may require local installation of the operating system. If this is not the case, the operating system should be factory-installed and have the most recent patches applied.

Support Level / Term – The operating system support level must be consistent with the criticality of the server and match hardware service level; term is three years with two option years unless VA has a standing enterprise software support agreement pertinent OS.

EVALUATION FACTORS

- Hardware support for the latest version of OS is beneficial.
- Installation of VA-supplied image is beneficial.

IMPLEMENTATION GUIDANCE

- UNIX requires exception justification and Solaris is the preferred UNIX product.
- Preference is for the latest versions of the operating system that are certified for implementation on the VA production network and supported by the hosted applications. If earlier versions are required due to compatibility limitations, these limitations should be documented for justification.

3.1.15 PLATFORM SOFTWARE / LICENSE

STANDARD

ID	***Secondary Attribute***	***Specification***
15	Multipath	Provides automated load balancing (all paths active) and fail-over; compatible with target storage array
	Data Backup	(optional) Matches requirements of the deployment location data center and SAN backup solution
	Monitoring Tool	Matches requirements of the deployment location data center
	Layered Framework	Defined by the application owner – meet license requirements for this server
	Server Management Tools	Matches requirements of the deployment location data center
	Availability / Recovery Tools	Matches the requirements for Persistent Computing standards applied to the hosted applications/services
	Security Tools	Follows Office of Information and Technology standards including compliance with FIPS, FISMA, and VA Directives.
	Virtual Management Software	Not required

EXPLANATION OF STANDARD

Multipath – Require failover capability with all paths active; Include requisite multipath software from appropriate storage vendor to provide failover and load-balancing capabilities.

Data Backup – Although this type of server primarily uses backup tools for server image backup, there may (optionally) be a need for data backup tools. A data backup tool/agent might be required by some hosted applications that have local database storage. In addition, some applications might have data stored on the SAN and is covered by the SAN backup solution that requires an agent on the server. For these servers, enterprise data backup tools are being evaluated and might lead to an enterprise standard. In the meantime, the tool selection is driven by each data center location, and must adhere to security/encryption policies. This software is installed and configured by VA and might utilize existing/enterprise licenses.

Monitoring Tool and Server Management Tool – These are the agents required by server monitoring & management tools or other monitoring tools – if agents are required. It is expected that these tools will largely be defined by the Enterprise Management Framework. The tools must meet the VA EMF standards/tools, or be able to feed information directly into the EMF tools. Until such standards are available, these tools must meet the data center standards where the tools are being placed. This software is installed and configured by VA and might utilize existing/enterprise licenses.

Availability / Recovery Tools – These include agents or other software for image backup and restoration tools, service replication tools, and fail-over tools. These will be defined in the Persistent Computing standards and by the hosted application's model for persistent computing. This software might be installed/configured through a service contract associated with the server purchase, or might be installed/configured by VA.

Security Tools – must follow Office of Information and Technology standards including compliance with FIPS, FISMA, and VA Directives, and be implemented in a way that meets Certification and Accreditation (C&A) requirements. VA Enterprise Security Solution Service (ESSS) can provide a review of proposed security tools and can be reached by contacting the Enterprise Solutions Security Service under OI&T Field Security Operations.

EVALUATION FACTORS

- Multipath – compatibility with a wide range of storage arrays / manufacturers is a benefit.

IMPLEMENTATION GUIDANCE

- This section is designed to provide guidance on what is typically purchased\installed on server platforms and should be used as a reference when making purchase\deployment decisions.

3.1.16 DATACENTER MANAGEMENT

STANDARD

ID	*Secondary Attribute*	*Specification*
16	Remote Keyboard/Video/Mouse	Ability to remotely connect to the server's external keyboard, video, and mouse ports through a networked KVM switch.

	Control	
	Remote Power Disconnect	Ability to remotely disconnect/reconnect server to power source

EXPLANATION OF STANDARD

Remote Keyboard/Video/Mouse Control – A dongle to attach the server to a networked KVM switch is required. Refer to the Datacenter Standard, Section xx

Remote Power Disconnect – Ability to remotely disconnect/reconnect power source to server through the control of individual receptacles. Refer to Datacenter Standards, Section xx.

EVALUATION FACTORS

- Ability to remotely update device firmware is beneficial.
- Accessibility via web browser is beneficial – should support Microsoft Internet Explorer.

IMPLEMENTATION GUIDANCE

3.2 TYPICAL WORKLOAD **(CLASS B)**

3.2.1 PROCESSOR

STANDARD

ID	***Secondary Attribute***	***Specification***
1	Type	x86_64 (e.g., Intel Xeon, AMD Opteron)
	Socket Count	Minimum required to meet Performance Benchmark standard
	Core Count	Amount required to meet Performance Benchmark standard
	Cache	Minimum total 2MB L2 Cache on chip (6MB or greater L3 Cache required for transactional servers)
	Virtualization Aware	Not Required

EXPLANATION OF STANDARD

Type – open/industry standard components.

Socket Count – minimize due to licensing costs per socket, have minimum count for performance/capacity.

Core Count – minimum amount expected for performance/capacity level is quad-core, more can be better. However, any amount that meets the Performance Benchmark specification is sufficient.

Cache – minimum expected for class of processor; low-power options might use lower amounts of cache.

EVALUATION FACTORS

- Currency of processor – most recent family and speed of processor is beneficial.
- Higher amounts of cache and cores are beneficial.
- Open processor slots or ability to enable additional processors for future expansion could be beneficial in larger configurations.

IMPLEMENTATION GUIDANCE

- It is recommended to have a Socket Count of two in order to minimize licensing costs that are calculated on a per socket basis. Exceptions for higher socket count should have justification documented and should consider both performance and cost.

3.2.2 PERFORMANCE

STANDARD

ID	***Secondary Attribute***	***Specification***
2	Performance Benchmark	SPEC CPU2006 Integer Rate Base value >= 200

EXPLANATION OF STANDARD

This SPEC_Int rate is represented by a large number of server platforms. Performance requirement is largely dependent on the application's workload and compute-resource consumption profile. The architecture of this server tier may provide sufficient horizontal scaling to accommodate larger workloads, especially with minimum server counts required for redundancy and limit of single-server impact. This specification is a starting point for a "typical" medium-workload application-server environment based upon review of existing tested systems in the VA environment and their capabilities represented with newer server offerings. This specification should be adjusted to meet the known workload of target hosted applications and the target architecture for its server tier.

EVALUATION FACTORS

- Higher benchmark rating value is beneficial.

IMPLEMENTATION GUIDANCE

3.2.3 MEMORY

STANDARD

ID	Secondary Attribute	Specification
3	Type	Compatible with CPU with full error correction capability including ECC; all memory modules must be of the same type and size.
	Total Memory	Minimum 48GB usable
	Speed	Minimum - match operational CPU and bus speed required to meet the Performance Benchmark requirement

EXPLANATION OF STANDARD

Type – Memory has to be highly reliable – ECC is the expected feature to allow higher levels of reliability. RDIMM is more expandable/scalable and provides additional reliability features (e.g., more error-checking features) while consuming more power (about one watt per chip) and costing more. In general, RDIMM is recommended with high memory requirements and higher availability requirements.

Total Memory – Memory requirements depend on application needs. The standard must meet the minimum requirement for memory intensive applications that could be run on this class of server. Using WebLogic as an example, minimum expected is 2GB-4GB per CPU core (as per Java configuration guidelines). With current VA application designs each JVM requires at least 4GB of memory; more if 64 bit JVMs are used. For a typical dual-socket quad-core server running WebLogic, the minimum expected requirement is therefore 48GB which would allow up to 12 JVMs. Usable memory value indicates the possibility of RAID or mirrored memory for additional redundancy. When using memory configurations above the minimum, internal storage capacity must be adjusted to support page/swap and dump requirements. This should be calculated using the formula: (2XRAM=page/swap size) + (1XRAM=DUMP) + (20GB for OS)

Speed **–** At least one operational speed of the memory must match the highest speed capability of the information bus used to retrieve memory for the CPU in order to maximize the investment into the CPU. Features can allow for step-down of speed correlated with workload consumption (power-saving feature).

EVALUATION FACTORS

- Additional memory is beneficial
- Higher density chips while avoiding a decrease in memory bus speed is preferred.
- Speed of memory takes precedence over density as long as capacity is met

IMPLEMENTATION GUIDANCE

- RDIMM is recommended for high memory requirements and higher availability requirements.

3.2.4 INTERNAL STORAGE

STANDARD

ID	*Secondary Attribute*	*Specification*
4	Type	SAS RAID controller supporting SAS drives and RAID/hot-spare features specified for this server
	Quantity of Drives	Minimum three
	RAID Configuration	Minimally require 2 disks in RAID1, plus 1 as hot spare, for page/swap, dump file, and options operating system functional role. Additional local storage needs (e.g., "temp file" storage for a transaction server or standalone storage configurations) are satisfied by additional drives in RAID level 1, 5, or 10 configuration, with a hot spare which can be shared with the page/swap disk's hot spare.
	Drive Speed	Minimum 10K RPM
	Drive Capacity	Minimum 300GB usable storage capacity
	Disk Subsystem Performance	The disk raid group must meet or exceed the performance levels specified for tests "Transaction Rate" and "Throughput Rate" Validation will be incorporated in user acceptance phase.
	Controller Cache	Minimum 256MB
	Quantity of Controllers	Minimum of one

EXPLANATION OF STANDARD

Type – SAS is preferred over SATA for the following reasons: 1) SAS uses the SCSI command set which provides better error reporting and recovery techniques than does SATA, 2) SATA throughput can be degraded on SAS adapters that use the Serial Tunneling Protocol (STP) to communicate with SATA targets, and 3) because they are engineered for continuous duty cycles and longer MTBFs, SAS drives are an accepted industry standard for enterprise server solutions. Solid state drives are beneficial due to power, cooling, performance, and reliability, but are expensive and currently are only used sparingly in external storage systems.

Quantity & RAID Configuration – requires performance for a page/swap disk and dump file, with possible additional uses; ability to continue with a drive failure (e.g., RAID1) and restore to this state with an immediately available drive (hot spare). For high performance functions (including page/swap disk), RAID1 is preferred over parity protection due to overhead of calculating parity. Although additional drives may help spread I/O across more drives for enhanced performance, additional drives also add to the cost, maintenance, and power consumption on the server. Therefore, additional drives should only be considered when they are required for performance or capacity reasons. The optimal configuration uses the fewest quantity of drives to meet the performance and reliability requirements. Additional drives are needed for additional storage needs such as

transaction server “temp file” storage or a standalone storage configuration which is provided on a separate disk per industry best practice guidance.

Drive Speed – Minimum RPM for this class of server & storage is 10K.

Drive Capacity –300GB minimum usable storage capacity is sufficient to support an operating system and/or swap and log files. This amount represents the expected minimum required for page/swap file, dump file, and optional system disk storage needs. When using memory configurations above the minimum, internal storage capacity must be adjusted to support page/swap and dump requirements. This should be calculated using the formula: (2XRAM=page/swap size) + (1XRAM=DUMP) + (20GB for OS)

Disk Subsystem Performance – The disk raid group must meet or exceed the performance levels specified below for tests “Transaction Rate” and “Throughput Rate” as described in APPENDIX G.

- Transaction Rate = 500+ IOPS
- Throughput Rate = 50+ MBPS

Controller Cache – minimum expected value for typical controllers for this class of server.

Quantity of Controllers – limited value to have more than one with only one RAID configuration; might be beneficial for more than two RAID sets if performance requires it; current technology offerings limit the ability to fail services over from one controller to another without manual intervention – future technology offerings such as dual-domain active/active configurations in SAS controllers & drives provide this capability

EVALUATION FACTORS

- Higher storage capacity is beneficial
- Higher RPM is beneficial for drive platters
- The optimal configuration uses the fewest quantity of drives to meet the performance and reliability requirements.
- Solid-state drives would be beneficial
- Higher throughput capability is beneficial
- Higher IOPS capability is beneficial
- More controllers can be beneficial
- More cache is beneficial
- Battery backup of cache is beneficial
- Support for RAID levels 0, 1, 5, 6, 0+1, and/or 1+0 is beneficial
- Separate hot spares for separate RAID groups is beneficial.

IMPLEMENTATION GUIDANCE

- SAS interface type is recommended. Battery backup of cache is recommended.

3.2.5 EXTERNAL STORAGE INTERFACE

STANDARD

ID	*Secondary Attribute*	*Specification*
5	Type	Fiber-channel with duplex LC connectors, CPU bus type is PCI-E Or Ethernet matching connector type of storage-dedicated network in data center. TOE / TCP checksum offload required.
	Port Count	Minimum of two
	Bandwidth	Minimum 4Gbps for optical or 1Gbps for copper; must meet or exceed SAN fabric requirements
	Compatibility	Support storage arrays at deployment location; supported by operating system and multipath drivers specified for this server
	SAN Boot Capability	BIOS support for SAN boot
	Blade Chassis Component (if applicable)	Dual embedded switches
	Hardware Redundancy	Supports connecting redundant ports configured to separate switches on the SAN. Minimum two adapters with minimum one port per adapter. Support for link aggregation.

EXPLANATION OF STANDARD

- Type – fiber channel and Ethernet are the vast majority of investment for connections used in storage-dedicated networks in VA data centers, and exceptions should be justified including impact to existing infrastructure investment. Typical Ethernet connector types are RJ-45 for copper and LC for optical. When Ethernet is used, TOE / TCP checksum offload is required. Drivers are more readily available for Windows than Linux servers.
- Port Count – minimum required for port-level redundancy / load-balancing
- Bandwidth – 4Gbps is standard for current investment of optical fabrics in the storage systems and infrastructure in VA data centers and matches the minimum current industry standard; similarly 1Gbps is standard for current investments and minimum current industry practices when using copper-based storage fabrics.
- Compatibility – Support storage subsystems at deployment locations. Check adapter compatibility for storage at deployment location.
- Blade Chassis Component – A primary benefit of blade servers is their ability to reduce datacenter cabling. Dual fiber-channel switches (or Ethernet if applicable) are required. Pass-thru configurations require an exception. Each blade chassis shall have redundant sets of embedded switches to provide independent SAN

connections to each blade. Each embedded switch set shall have the ability to configure redundant and/or trunked ISL/uplink ports. Minimum number of uplink ports in chassis is two times the number of embedded switches. Refer to Storage Standards, Section xx.

- Hardware Redundancy – Fail-over and load-balancing are functions of the multipath tool which is covered in section 3.2.16

EVALUATION FACTORS

- Redundancy across physically independent interfaces is beneficial
- Support for 8Gbps optical or 10Gbps copper bandwidth is beneficial

IMPLEMENTATION GUIDANCE

- For a server with high criticality of SAN storage connectivity, redundant adapter cards are recommended.
- Interface for iSCSI can be termed an HBA interface or a NIC interface. Where higher performance is a concern, the HBA interface is recommended.
- Bandwidth spread across multiple ports on independent cards may be required for performance reasons

3.2.6 SERVER COMMUNICATIONS INTERFACE

STANDARD

ID	***Secondary Attribute***	***Specification***
6	Type	Ethernet matching connector type for network in data center
	Port Count	Minimum of 2 ports; at least 2 more if private cluster interconnect is required
	Bandwidth	Minimum 1Gbps
	Hardware Redundancy	Supports connecting redundant ports configured to separate switches on the LAN; supports redundant ports (may include embedded ports) for each interface function (e.g., public network function and cluster interconnect function)
	Blade Chassis Component (if applicable)	Dual embedded switches

EXPLANATION OF STANDARD

Type – Ethernet is the vast majority of investment for connections used in data center networks in VA, and exceptions should be justified including impact to existing infrastructure investment. Typical Ethernet connector types are RJ-45 for copper and LC for optical with a future trend towards copper only.

Port Count – base set of 2 ports are for general “public” Ethernet; other specific interfaces may be required depending on the profile of the workload/application. Cluster interconnects may need 2 or more ports, depending

on the amount of cluster traffic (e.g., Oracle clusters send data over the cluster interconnect, simple Microsoft clustering only send "heartbeat" traffic).

Bandwidth – expected standard interface on network switches is 1Gbps. There is a potential for 10Gbps Ethernet.

Hardware Redundancy – embedded ports count as one "card" which is sufficient for this class of server except where additional ports are required. If additional ports are required, all interface uses are spread across two "cards" (including at least one add-on NIC). The goal is physical separation of the chipset/ASIC used on the redundant port, for each function. Support for "simple failover" (with a single IP address) and independent usage (with multiple IP addresses) is required.

Blade Chassis Component – Where applicable, blade-server chassis should be configured with two switches to limit port and cabling needs external to the server, unless there is a specific workload/application requirement for high throughput that requires pass-through capability.

EVALUATION FACTORS

- Additional cards can be beneficial
- Support for TCP Offload Engine is beneficial
- Support for active/active load balancing is beneficial

IMPLEMENTATION GUIDANCE

- One or two additional ports are recommended for network backups if the impact of backup traffic may affect other services on the "public" network. One port is sufficient if only one port is active and uses another port for fail-over.
- TCP Offload Engine (TOE) is preferred for all servers. Drivers are more readily available for Windows than Linux servers.
- If there is a specific workload/application requirement for high throughput that requires pass-through capability on a blade-server chassis, then this option should be configured, but the chassis switch is preferred otherwise.
- Bandwidth spread across multiple ports on independent cards may be required for performance reasons

3.2.7 REMOVABLE MEDIA DEVICE

STANDARD

ID	*Secondary Attribute*	*Specification*
7	Optical Drive	(optional) CD/DVD drive – minimum 24x speed
	USB	USB v2.0 port

EXPLANATION OF STANDARD

The functional requirement supported by this standard is to provide a media transfer mechanism to upload patch and software/firmware installation, upload diagnostic tools, and (with read/write capability) to download

diagnostic information. Manufacturers are going toward a trend of using USB flash drives for sending patch/upgrade/firmware distributions. Therefore, the requirement is to provide both CD/DVD and USB flash drive capabilities. Note that security restrictions or concerns need to be addressed before using removable media.

The optical drive is optional because small form factor (e.g., blade) servers might not allow this type of component. These small form factor servers do, however, have the ability to support USB flash drives.

The type of drive specified is the typical expected minimum specification and type.

EVALUATION FACTORS

- Having an optical drive is beneficial.
- Faster speeds and/or Read-write capability is beneficial (additional security checks may be required for read/write capability).

IMPLEMENTATION GUIDANCE

- Preferred to provide removable media device for patch and software installation options; but small form factor (e.g., blade) servers might use other options.

3.2.8 POWER

STANDARD

ID	***Secondary Attribute***	***Specification***
8	Redundancy	N+1 redundancy on power supply
	Voltage	115-208V input voltage on power supplies
	Cord Type	IEC
	Power Efficiency	Until such time that there are Energy Star ratings available to most server classes, power efficiency should be consistent with industry trends.
	Power Consumption Documentation	Vendor-supplied data for power consumption of specified configuration at 100% load, “typical” active usage, and at idle.

EXPLANATION OF STANDARD

Redundancy – server must continue to operate if and when a power supply fails in order to enhance availability.

Voltage and cord type – driven by data center standards, 208V can more efficiently use power from utility

Power Efficiency – Certifications for power efficiency include: 80-plus (Dell & HP certify through them, but IBM does not), and Energy Star (still forming the standard for servers, but blade servers will be separate standard). The EPA establishes Energy Star standards – tier 2 appears to be the four-socket type of server while tier 1 appears to

be the dual-socket server types. Some server manufacturers implement power efficiency management features including step-down of power consumption during low resource-consumption states.

Power Consumption Documentation – Preferred documentation is Energy Star data sheet and/or SPECpower_ssj2008 published results.

EVALUATION FACTORS

- Power management/economy and reporting/analysis features are beneficial.
- Lower power consumption rating at 100% utilization per workload capacity (in terms of SPECint_rate value) is beneficial.

IMPLEMENTATION GUIDANCE

- Cord type of IEC-C13 is preferred for most classes of rack-mount servers

3.2.9 COOLING FAN

STANDARD

ID	***Secondary Attribute***	***Specification***
9	Redundancy	Minimum N+1 redundancy

EXPLANATION OF STANDARD

- Redundancy – server must continue to operate if and when a fan fails in order to enhance availability.

EVALUATION FACTORS

- Additional fans or separation of fans into multiple cooling zones is beneficial.
- Lower total decibel rating on the fans is beneficial.

IMPLEMENTATION GUIDANCE

3.2.10 OUT OF BAND MANAGEMENT

STANDARD

ID	Secondary Attribute	Specification
10	Type	Remote command-line and console-level access utilizing dedicated network interface
	Security	Secure IP-based remote management that complies with all VA security requirements
	Remote Power Control	Ability to remotely power on/off/reset server

EXPLANATION OF STANDARD

Required dedicated network interface is required outside of the other network interfaces specified in section 3.2.7.

Based on data center environment, operational needs, and minimum requirements that are typically satisfied through a wide variety of servers. Includes access for diagnostic capability.

Remote Power Control – Ability to power on/off/reset through server based management.

EVALUATION FACTORS

- Ability to remotely mount a drive or ISO is beneficial. This can be used for software, firmware and OS updates using remote drive mounting, and it minimizes the need for local optical drive.
- Active Directory integration for authentication is beneficial.
- Role-based access control is beneficial.
- Accounting capability is beneficial.
- Strong password compliance is beneficial.
- Accessibility via web browser is beneficial – should support Microsoft Internet Explorer.
- Support for Secure Shell (SSH) connections is beneficial – should be FIPS 140-2 compliant.
- Ability to remotely identify server with visual indicator (e.g., indicator light) is beneficial.

IMPLEMENTATION GUIDANCE

3.2.11 SERVER HARDWARE VENDOR SUPPORT

STANDARD

ID	Secondary Attribute	Specification
11	Type	Match service level requirement for hosted applications; mission-critical level

		support shall include 24x7 coverage 365 days/year, less than 1 hour initial engineer-level response time, 4-hour on-site response time for emergency dispatches, and 8-hour time-to-repair
	Term Length	Minimum of three years with two additional option years
	Keep Your Hard Drive	All storage drives are kept by VA in the event of warranty/service replacement

EXPLANATION OF STANDARD

Type – the level of support matches the criticality level of the hosted services. Mission-critical level is defined in this standard, and has been shown to be accommodated by major server vendors. Other levels will have to be defined to match the business expectations of that criticality level. A non-critical example would be 8 business hours/weekday phone coverage with next-day response and repair. Access to original server manufacturer support with the option to escalate to senior technicians at VA discretion is required.

Term – some components might only allow three years of support on an initial contract, but option years must be available to extend that to the expected lifetime of the system which is nominally five years.

Keep Your Hard Drive – This is a security requirement that is now a de-facto standard in VA.

EVALUATION FACTORS

- Lower on-site response time is beneficial.
- Lower initial "engineer level" contact response time is beneficial.
- Lower time-to-repair is beneficial.
- Vendor-supplied components stocked as spares near, or at, facility is beneficial.
- Penalty clauses for vendor not meeting support contract provides benefit.
- Allowance for optional parts-delivery/customer-installation of hot swappable components, memory, and drop-in cards beneficial at the VA's option.
- Access to electronic models of equipment being proposed is beneficial. Because electronic models will be used with CAD and visual design applications for datacenter planning, three dimensional models are preferred.

IMPLEMENTATION GUIDANCE

- It is preferred to have vendor-supplied total system replacements able to ship out to the site within 24 hours via overnight shipment means.

3.2.12 HARDWARE MANAGEMENT SOFTWARE

STANDARD

ID	***Secondary Attribute***	***Specification***
12	Type	Agent or agent-less server management tool accessible through SNMP

	Automated Notification	Hardware events including exceptions, diagnostics, and failures, shall be exposed through SNMP with documented MIBs
	Shared Repository	Allows uploading all information collected by the tool into shared repository using ODBC or JBDC in a manner that preserves data fields for the diagnostic information (e.g., date/time, error code, module, description, system identification, status, system configuration)
	Support Level	Support level of management software must match support level of server hardware

EXPLANATION OF STANDARD

The tool should allow management of the hardware through a variety of means that interface with SNMP, and must be fully documented with MIBs for all relevant data (hardware events). Integration with VA's Enterprise Exception Log Service (EELS) is a consideration and is enabled through SNMP interfacing.

Ability to access event logs through database connectivity (JDBC or ODBC) is needed for future Enterprise Management Framework tools.

Service could be provided through BIOS feature, OS-level features, or other layered features, and must provide the MIB documentation for accessing the information.

EVALUATION FACTORS

- Ability to integrate with a variety of industry enterprise-level system management tools is beneficial.
- Inclusion of an enterprise-level component with shared repository and correlation analysis features is beneficial.
- Ability to provide management of agent-less systems is beneficial.

IMPLEMENTATION GUIDANCE

- Support for SNMPv3 is preferred.
- A solution design that provides secure connections outside the physical facility is preferred.
- Automated vendor notification of failure, or pre-failure activity, to initiate vendor remediation is preferred.

3.2.13 RACK INFRASTRUCTURE COMPATIBILITY

STANDARD

ID	*Secondary Attribute*	*Specification*
13	Rack Unit Measurement	1U or 2U for rack-mount servers; blade implementations will be evaluated on an individual basis.
	Rail Type	Tool-less square-hole sliding

	Cable Management	Side-reversible for non-blade solutions

EXPLANATION OF STANDARD

Rack Unit Measurement – For this class of server, occupying 4U (or two blade slots) should not be necessary; 1 slot in a half-height blade chassis is fairly equivalent to a 1U rack-mount and 1 slot in a full-height blade chassis is fairly equivalent to a 2U rack-mount. It is expected that this class of server will be a 2U rack mount or single slot full-height blade server.

Rail Type – server must have rail adapters if needed to fit the generic non-proprietary type of rack specified in this standard.

Rack infrastructure standards must match the data center equipment rack standards.

EVALUATION FACTORS

- Lower occupied rack space (per workload) is beneficial

IMPLEMENTATION GUIDANCE

3.2.14 OPERATING SYSTEM

STANDARD

ID	***Secondary Attribute***	***Specification***
14	Type	Linux preferred based on federal requirement to utilize open source operating systems, Windows acceptable, all must VA approved operating systems and compatible with hardware.
	Version	Current target version of Linux or Windows per VA TRM
	Vendor-Installed	Depends on data center policy; default is factory-installed with default settings and most recent patch level
	Support Level / Term	Must match hardware service level; term is three years with two option years unless VA has a standing enterprise software support agreement pertinent OS.

EXPLANATION OF STANDARD

Type – Linux is preferred as the most “open” type of option, but Windows is also acceptable as an industry-wide supported option. If UNIX is required Solaris is the preferred UNIX product. Solaris is preferred due to the “open” features and high level of government security certification.

Version – Operating system build, distribution, and version must be listed in the VA TRM.

Vendor-Installed – Data center policy may require local installation of the operating system. If this is not the case, the operating system should be factory-installed and have the most recent patches applied.

Support Level / Term – The operating system support level must be consistent with the criticality of the server and match hardware service level; term is three years with two option years unless VA has a standing enterprise software support agreement pertinent OS.

EVALUATION FACTORS

- Hardware support for the latest version of OS is beneficial.
- Installation of VA-supplied image is beneficial.

IMPLEMENTATION GUIDANCE

- UNIX requires exception justification and Solaris is the preferred UNIX product.
- Preference is for the latest versions of the operating system that are certified for implementation on the VA production network and supported by the hosted applications. If earlier versions are required due to compatibility limitations, these limitations should be documented for justification.

3.2.15 PLATFORM SOFTWARE / LICENSE

STANDARD

ID	***Secondary Attribute***	***Specification***
15	Multipath	Provides automated load balancing (all paths active) and fail-over; compatible with target storage array
	Data Backup	(optional) Matches requirements of the deployment location data center and SAN backup solution
	Monitoring Tool	Matches requirements of the deployment location data center
	Layered Framework	Defined by the application owner – meet license requirements for this server
	Server Management Tools	Matches requirements of the deployment location data center
	Availability / Recovery Tools	Matches the requirements for Persistent Computing standards applied to the hosted applications/services
	Security Tools	Follows Office of Information and Technology standards including compliance with FIPS, FISMA, and VA Directives.
	Virtual Management Software	Not Required

EXPLANATION OF STANDARD

Multipath – Require failover capability with all paths active; Include requisite multipath software from appropriate storage vendor to provide failover and load-balancing capabilities.

Data Backup – Although this type of server primarily uses backup tools for server image backup, there may (optionally) be a need for data backup tools. A data backup tool/agent might be required by some hosted applications that have local database storage. In addition, some applications might have data stored on the SAN and is covered by the SAN backup solution that requires an agent on the server. For these servers, enterprise data backup tools are being evaluated and might lead to an enterprise standard. In the meantime, the tool selection is driven by each data center location, and must adhere to security/encryption policies. This software is installed and configured by VA and might utilize existing/enterprise licenses.

Monitoring Tool and Server Management Tool – These are the agents required by server monitoring & management tools or other monitoring tools – if agents are required. It is expected that these tools will largely be defined by the Enterprise Management Framework. The tools must meet the VA EMF standards/tools, or be able to feed information directly into the EMF tools. Until such standards are available, these tools must meet the data center standards where the tools are being placed. This software is installed and configured by VA and might utilize existing/enterprise licenses.

Availability / Recovery Tools – These include agents or other software for image backup and restoration tools, service replication tools, and fail-over tools. These will be defined in the Persistent Computing standards and by the hosted application's model for persistent computing. This software might be installed/configured through a service contract associated with the server purchase, or might be installed/configured by VA.

Security Tools – must follow Office of Information and Technology standards including compliance with FIPS, FISMA, and VA Directives, and be implemented in a way that meets Certification and Accreditation (C&A) requirements. VA Enterprise Security Solution Service (ESSS) can provide a review of proposed security tools and can be reached by contacting the Enterprise Solutions Security Service under OI&T Field Security Operations.

EVALUATION FACTORS

- Multipath – compatibility with a wide range of storage arrays / manufacturers is a benefit.

IMPLEMENTATION GUIDANCE

- .This section is designed to provide guidance on what is typically purchased\installed on server platforms and should be used as a reference when making purchase\deployment decisions.

3.2.16 DATACENTER MANAGEMENT

STANDARD

ID	*Secondary Attribute*	*Specification*
16	Remote Keyboard/Video/Mouse	Ability to remotely connect to the server's external keyboard, video, and mouse ports through a networked KVM switch.

	Control	
	Remote Power Disconnect	Ability to remotely disconnect/reconnect server to power source

EXPLANATION OF STANDARD

Remote Keyboard/Video/Mouse Control – A dongle to attach the server to a networked KVM switch is required. Refer to the Datacenter Standard, Section xx

Remote Power Disconnect – Ability to remotely disconnect/reconnect power source to server through the control of individual receptacles. Refer to Datacenter Standards, Section xx.

EVALUATION FACTORS

- Ability to remotely update device firmware is beneficial.
- Accessibility via web browser is beneficial – should support Microsoft Internet Explorer.

IMPLEMENTATION GUIDANCE

3.3 HEAVY WORKLOAD (**CLASS A**)

3.3.1 PROCESSOR

STANDARD

ID	***Secondary Attribute***	***Specification***
1	Type	x86_64 (e.g., Intel Xeon, AMD Opteron)
	Socket Count	Minimum required to meet Performance Benchmark standard
	Core Count	Amount required to meet Performance Benchmark standard
	Cache	Minimum total 2MB L2 Cache on chip (6MB or greater L3 Cache required for transactional servers)
	Virtualization Aware	Required to facilitate live migration

EXPLANATION OF STANDARD

Type – open/industry standard components.

Socket Count – minimize due to licensing costs per socket, have minimum count for performance/capacity.

Core Count – minimum amount expected for performance/capacity level is quad-core, more can be better. However, any amount that meets the Performance Benchmark specification is sufficient.

Cache – minimum expected for class of processor; low-power options might use lower amounts of cache.

Virtualization Aware – CPU manufacturers offer technology that allows easy migration of running virtual guests from one physical host to another. Servers in this class must provide that functionality.

EVALUATION FACTORS

- Currency of processor – most recent family and speed of processor is beneficial.
- Higher amounts of cache and cores are beneficial.
- Open processor slots or ability to enable additional processors for future expansion could be beneficial in larger configurations.

IMPLEMENTATION GUIDANCE

- It is recommended to have a Socket Count of four or less in order to minimize licensing costs that are calculated on a per socket basis. Exceptions for higher socket count should have justification documented and should consider both performance and cost.

3.3.2 PERFORMANCE

STANDARD

ID	***Secondary Attribute***	***Specification***
2	Performance Benchmark	SPEC CPU2006 Integer Rate Base value >= 250

EXPLANATION OF STANDARD

This SPEC_Int rate is represented by a large number of server platforms. Performance requirement is largely dependent on the application's workload and compute-resource consumption profile. This specification is a starting point for a "heavy duty" high-workload transactional or virtual server environment based upon review of existing tested systems in the VA environment and their capabilities represented with newer server offerings. This specification should be adjusted to meet the known workload of target hosted applications and the target architecture for its server tier.

EVALUATION FACTORS

- Higher benchmark rating value is beneficial.

IMPLEMENTATION GUIDANCE

3.3.3 MEMORY

STANDARD

ID	*Secondary Attribute*	*Specification*
3	Type	Compatible with CPU with full error correction capability including ECC; all memory modules must be of the same type and size.
	Total Memory	Minimum 128GB usable
	Speed	Minimum - match operational CPU and bus speed required to meet the Performance Benchmark requirement

EXPLANATION OF STANDARD

Type – Memory has to be highly reliable – ECC is the expected feature to allow higher levels of reliability. RDIMM is more expandable/scalable and provides additional reliability features (e.g., more error-checking features) while consuming more power (about one watt per chip) and costing more. In general, RDIMM is recommended with high memory requirements and higher availability requirements.

Total Memory – Memory requirements depend on application needs. The standard must meet the minimum requirement for memory intensive applications that could be run on this class of server. Using virtual hosting as an example, the minimum standard would allow for 4 to 8 virtual guests configured with 16GB to 32GB each. Usable memory value indicates the possibility of RAID or mirrored memory for additional redundancy. This class of server should provide at least 8 environments in a medium application environment. When using memory configurations above the minimum, internal storage capacity must be adjusted to support page/swap and dump requirements. This should be calculated using the formula: (2XRAM=page/swap size) + (1XRAM=DUMP) + (20GB for OS)

Speed – At least one operational speed of the memory must match the highest speed capability of the information bus used to retrieve memory for the CPU in order to maximize the investment into the CPU. Features can allow for step-down of speed correlated with workload consumption (power-saving feature).

EVALUATION FACTORS

- Additional memory is beneficial
- Higher density chips while avoiding a decrease in memory bus speed is preferred.
- Speed of memory takes precedence over density as long as capacity is met

IMPLEMENTATION GUIDANCE

- RDIMM is recommended for high memory requirements and higher availability requirements.

3.3.4 INTERNAL STORAGE

STANDARD

ID	Secondary Attribute	Specification
4	Type	SAS RAID controller supporting SAS drives and RAID/hot-spare features specified for this server
	Quantity of Drives	Minimum three
	RAID Configuration	Minimally require 2 disks in RAID1, plus 1 as hot spare, for page/swap, dump file, and options operating system functional role. Additional local storage needs (e.g., "temp file" storage for a transaction server or standalone storage configurations) are satisfied by additional drives in RAID level 1, 5, or 10 configuration, with a hot spare which can be shared with the page/swap disk's hot spare. When this class of server is configured as a transaction server, a separate RAID controller or second channel on the same controller is required for the "temp file" RAID group
	Drive Speed	Minimum 10K RPM
	Drive Capacity	Minimum 450GB usable storage capacity
	Disk Subsystem Performance	The disk raid group must meet or exceed the performance levels specified for tests "Transaction Rate" and "Throughput Rate" Validation will be incorporated in user acceptance phase.
	Controller Cache	Minimum 256MB
	Quantity of Controllers	Minimum of one

EXPLANATION OF STANDARD

Type – SAS is preferred over SATA for the following reasons: 1) SAS uses the SCSI command set which provides better error reporting and recovery techniques than does SATA, 2) SATA throughput can be degraded on SAS adapters that use the Serial Tunneling Protocol (STP) to communicate with SATA targets, and 3) because they are engineered for continuous duty cycles and longer MTBFs, SAS drives are an accepted industry standard for enterprise server solutions. Solid state drives are beneficial due to power, cooling, performance, and reliability, but are expensive and currently are only used sparingly in external storage systems.

Quantity & RAID Configuration – requires performance for a page/swap disk and dump file, with possible additional uses; ability to continue with a drive failure (e.g., RAID1) and restore to this state with an immediately available drive (hot spare). For high performance functions (including page/swap disk), RAID1 is preferred over parity protection due to overhead of calculating parity. Although additional drives may help spread I/O across more drives for enhanced performance, additional drives also add to the cost, maintenance, and power consumption on the server. Therefore, additional drives should only be considered when they are required for performance or capacity reasons. The optimal configuration uses the fewest quantity of drives to meet the

performance and reliability requirements. Additional drives are needed for additional storage needs such as transaction server "temp file" storage or a standalone storage configuration which is provided on a separate disk per industry best practice guidance.

Drive Speed – Minimum RPM for this class of server & storage is 10K.

Drive Capacity – 450GB minimum usable storage capacity is sufficient to support an operating system and/or swap and log files. This amount represents the expected minimum required for page/swap file, dump file, and optional system disk storage needs. When using memory configurations above the minimum, internal storage capacity must be adjusted to support page/swap and dump requirements. This should be calculated using the formula: (2XRAM=page/swap size) + (1XRAM=DUMP) + (20GB for OS)

Disk Subsystem Performance – The disk raid group must meet or exceed the performance levels specified below for tests "Transaction Rate" and "Throughput Rate" as described in APPENDIX G.

- Transaction Rate = 500+ IOPS
- Throughput Rate = 50+ MBPS

Controller Cache – minimum expected value for typical controllers for this class of server.

Quantity of Controllers – limited value to have more than one with only one RAID configuration; might be beneficial for more than two RAID sets if performance requires it; current technology offerings limit the ability to fail services over from one controller to another without manual intervention – future technology offerings such as dual-domain active/active configurations in SAS controllers & drives provide this capability

EVALUATION FACTORS

- Higher storage capacity is beneficial
- Higher RPM is beneficial for drive platters
- The optimal configuration uses the fewest quantity of drives to meet the performance and reliability requirements.
- Solid-state drives would be beneficial
- Higher throughput capability is beneficial
- Higher IOPS capability is beneficial
- More controllers can be beneficial
- More cache is beneficial
- Battery backup of cache is beneficial
- Support for RAID levels 0, 1, 5, 6, 0+1, and/or 1+0 is beneficial
- Separate hot spares for separate RAID groups is beneficial.

IMPLEMENTATION GUIDANCE

- SAS interface type is recommended. Battery backup of cache is recommended.

3.3.5 EXTERNAL STORAGE INTERFACE

STANDARD

ID	*Secondary Attribute*	*Specification*
5	Type	Fiber-channel with duplex LC connectors, CPU bus type is PCI-E Or Ethernet matching connector type of storage-dedicated network in data center. TOE / TCP checksum offload required.
	Port Count	Minimum of 2 independent cards with a minimum of 2 ports each
	Bandwidth	Minimum 4Gbps for optical or 1Gbps for copper; must meet or exceed SAN fabric requirements
	Compatibility	Support storage arrays at deployment location; supported by operating system and multipath drivers specified for this server
	SAN Boot Capability	BIOS support for SAN boot
	Blade Chassis Component (if applicable)	Dual embedded switches
	Hardware Redundancy	Supports connecting redundant ports configured to separate switches on the SAN. Minimum two adapters with minimum one port per adapter. Support for link aggregation.

EXPLANATION OF STANDARD

- Type – fiber channel and Ethernet are the vast majority of investment for connections used in storage-dedicated networks in VA data centers, and exceptions should be justified including impact to existing infrastructure investment. Typical Ethernet connector types are RJ-45 for copper and LC for optical. When Ethernet is used, TOE / TCP checksum offload is required. Drivers are more readily available for Windows than Linux servers.
- Port Count – minimum required for port-level redundancy / load-balancing. Provides the flexibility to improve the throughput and performance without further hardware changes. Can initially configure with only 2 active. Potential benefit for separating the ports used for booting and data. Allows increased workload of multiple database servers in shared server environment.
- Bandwidth – 4Gbps is standard for current investment of optical fabrics in the storage systems and infrastructure in VA data centers and matches the minimum current industry standard; similarly 1Gbps is standard for current investments and minimum current industry practices when using copper-based storage fabrics.
- Compatibility – Support storage subsystems at deployment locations. Check adapter compatibility for storage at deployment location. Don't want to provide a list of brand names.

- Blade Chassis Component – A primary benefit of blade servers is their ability to reduce datacenter cabling. Dual fiber-channel switches (or Ethernet if applicable) are required. Pass-thru configurations require an exception. Each blade chassis shall have redundant sets of embedded switches to provide independent SAN connections to each blade. Each embedded switch set shall have the ability to configure redundant and/or trunked ISL/uplink ports. Minimum number of uplink ports in chassis is two times the number of embedded switches. Refer to Storage Standards, Section xx.
- Hardware Redundancy – Fail-over and load-balancing are functions of the multipath tool which is covered in section 3.3.16

EVALUATION FACTORS

- Redundancy across physically independent interfaces is beneficial
- Support for 8Gbps optical or 10Gbps copper bandwidth is beneficial
- Four independent cards with a minimum of 2 ports each is preferred.

IMPLEMENTATION GUIDANCE

- For a server with high criticality of SAN storage connectivity, redundant adapter cards are recommended.
- Interface for iSCSI can be termed an HBA interface or a NIC interface. Where higher performance is a concern, the HBA interface is recommended.
- Bandwidth spread across multiple ports on independent cards may be required for performance reasons

3.3.6 SERVER COMMUNICATIONS INTERFACE

STANDARD

ID	***Secondary Attribute***	***Specification***
6	Type	Ethernet matching connector type for network in data center
	Port Count	Minimum of 6 ports; more may be necessary depending on virtual infrastructure requirements
	Bandwidth	Minimum 1Gbps
	Hardware Redundancy	Supports connecting redundant ports configured to separate switches on the LAN; supports physically independent redundant ports including embedded ports for each interface function (e.g., public network function and cluster interconnect function)
	Blade Chassis Component (if applicable)	Dual embedded switches

EXPLANATION OF STANDARD

Type – Ethernet is the vast majority of investment for connections used in data center networks in VA, and exceptions should be justified including impact to existing infrastructure investment. Typical Ethernet connector types are RJ-45 for copper and LC for optical with a future trend towards copper only.

Port Count – when used in a virtual environment, a base set of 4 ports are used for virtual guests, 1 is for the console, and 1 for the live migration. Other specific interfaces may be required depending on the profile of the workload/application. When not used in a virtual environment, cluster interconnects may need 2 or more ports, depending on the amount of cluster traffic (e.g., Oracle clusters send data over the cluster interconnect, simple Microsoft clustering only send "heartbeat" traffic).

Bandwidth – expected standard interface on network switches is 1Gbps. There is a potential for 10Gbps Ethernet.

Hardware Redundancy – embedded ports count as one "card"; all interface uses are spread across two "cards" (including at least one add-on NIC). The goal is physical separation of the chipset/ASIC used on the redundant port, for each function. Support for "simple failover" (with a single IP address) and independent usage (with multiple IP addresses) is required.

Blade Chassis Component – Where applicable, blade-server chassis should be configured with two switches to limit port and cabling needs external to the server, unless there is a specific workload/application requirement for high throughput that requires pass-through capability.

EVALUATION FACTORS

- Additional cards can be beneficial
- Support for TCP Offload Engine is beneficial
- Support for active/active load balancing is beneficial

IMPLEMENTATION GUIDANCE

- One or two additional ports are recommended for network backups if the impact of backup traffic may affect other services on the "public" network. One port is sufficient if only one port is active and uses another port for fail-over.
- TCP Offload Engine (TOE) is preferred for all servers. Drivers are more readily available for Windows than Linux servers.
- If there is a specific workload/application requirement for high throughput that requires pass-through capability on a blade-server chassis, then this option should be configured, but the chassis switch is preferred otherwise.
- Bandwidth spread across multiple ports on independent cards may be required for performance reasons

3.3.7 REMOVABLE MEDIA DEVICE

STANDARD

ID	*Secondary Attribute*	*Specification*

7	Optical Drive	(optional) CD/DVD drive – minimum 24x speed
	USB	USB v2.0 port

EXPLANATION OF STANDARD

The functional requirement supported by this standard is to provide a media transfer mechanism to upload patch and software/firmware installation, upload diagnostic tools, and (with read/write capability) to download diagnostic information. Manufacturers are going toward a trend of using USB flash drives for sending patch/upgrade/firmware distributions. Therefore, the requirement is to provide both CD/DVD and USB flash drive capabilities. Note that security restrictions or concerns need to be addressed before using removable media.

The optical drive is optional because small form factor (e.g., blade) servers might not allow this type of component. These small form factor servers do, however, have the ability to support USB flash drives.

The type of drive specified is the typical expected minimum specification and type.

EVALUATION FACTORS

- Having an optical drive is beneficial.
- Faster speeds and/or Read-write capability is beneficial (additional security checks may be required for read/write capability).

IMPLEMENTATION GUIDANCE

- Preferred to provide removable media device for patch and software installation options; but small form factor (e.g., blade) servers might use other options.

3.3.8 POWER

STANDARD

ID	*Secondary Attribute*	*Specification*
8	Redundancy	N+1 redundancy on power supply
	Voltage	208V input voltage on power supply
	Cord Type	IEC
	Power Efficiency	Until such time that there are Energy Star ratings available to most server classes, power efficiency should be consistent with industry trends.
	Power Consumption Documentation	Vendor-supplied data for power consumption of specified configuration at 100% load, “typical” active usage, and at idle.

EXPLANATION OF STANDARD

Redundancy – server must continue to operate if and when a power supply fails in order to enhance availability.

Voltage and cord type – driven by data center standards, 208V can more efficiently use power from utility

Power Efficiency – Certifications for power efficiency include: 80-plus (Dell & HP certify through them, but IBM does not), and Energy Star (still forming the standard for servers, but blade servers will be separate standard). The EPA establishes Energy Star standards – tier 2 appears to be the four-socket type of server while tier 1 appears to be the dual-socket server types. Some server manufacturers implement power efficiency management features including step-down of power consumption during low resource-consumption states.

Power Consumption Documentation – Preferred documentation is Energy Star data sheet and/or SPECpower_ssj2008 published results.

EVALUATION FACTORS

- Power management/economy and reporting/analysis features are beneficial.
- Lower power consumption rating at 100% utilization per workload capacity (in terms of SPECint_rate value) is beneficial.

IMPLEMENTATION GUIDANCE

- Cord type of IEC-C13 is preferred for most classes of rack-mount servers

3.3.9 COOLING FAN

STANDARD

ID	***Secondary Attribute***	***Specification***
9	Redundancy	Minimum N+1 redundancy

EXPLANATION OF STANDARD

Redundancy – server must continue to operate if and when a fan fails in order to enhance availability.

EVALUATION FACTORS

- Additional fans or separation of fans into multiple cooling zones is beneficial.
- Lower total decibel rating on the fans is beneficial.

IMPLEMENTATION GUIDANCE

3.3.10 OUT OF BAND MANAGEMENT

STANDARD

ID	Secondary Attribute	Specification
10	Type	Remote command-line and console-level access utilizing dedicated network interface
	Security	Secure IP-based remote management that complies with all VA security requirements
	Remote Power Control	Ability to remotely power on/off/reset server

EXPLANATION OF STANDARD

Required dedicated network interface is required outside of the other network interfaces specified in section 3.2.7.

Based on data center environment, operational needs, and minimum requirements that are typically satisfied through a wide variety of servers. Includes access for diagnostic capability.

Remote Power Control – Ability to power on/off/reset through server based management.

EVALUATION FACTORS

- Ability to remotely mount a drive or ISO is beneficial. This can be used for software, firmware and OS updates using remote drive mounting, and it minimizes the need for local optical drive.
- Active Directory integration for authentication is beneficial.
- Role-based access control is beneficial.
- Accounting capability is beneficial.
- Strong password compliance is beneficial.
- Accessibility via web browser is beneficial – should support Microsoft Internet Explorer.
- Support for Secure Shell (SSH) connections is beneficial – should be FIPS 140-2 compliant.
- Ability to remotely identify server with visual indicator (e.g., indicator light) is beneficial.

IMPLEMENTATION GUIDANCE

3.3.11 SERVER HARDWARE VENDOR SUPPORT

STANDARD

ID	Secondary Attribute	Specification
11	Type	Match service level requirement for hosted applications; mission-critical level

		support shall include 24x7 coverage 365 days/year, less than 1 hour initial engineer-level response time, 4-hour on-site response time for emergency dispatches, and 8-hour time-to-repair
	Term Length	Minimum of three years with two additional option years
	Keep Your Hard Drive	All storage drives are kept by VA in the event of warranty/service replacement

EXPLANATION OF STANDARD

Type – the level of support matches the criticality level of the hosted services. Mission-critical level is defined in this standard, and has been shown to be accommodated by major server vendors. Other levels will have to be defined to match the business expectations of that criticality level. A non-critical example would be 8 business hours/weekday phone coverage with next-day response and repair. Access to original server manufacturer support with the option to escalate to senior technicians at VA discretion is required.

Term – some components might only allow three years of support on an initial contract, but option years must be available to extend that to the expected lifetime of the system which is nominally five years.

Keep Your Hard Drive – This is a security requirement that is now a de-facto standard in VA.

EVALUATION FACTORS

- Lower on-site response time is beneficial.
- Lower initial "engineer level" contact response time is beneficial.
- Lower time-to-repair is beneficial.
- Vendor-supplied components stocked as spares near, or at, facility is beneficial.
- Penalty clauses for vendor not meeting support contract provides benefit.
- Allowance for optional parts-delivery/customer-installation of hot swappable components, memory, and drop-in cards beneficial at the VA's option.
- Access to electronic models of equipment being proposed is beneficial. Because electronic models will be used with CAD and visual design applications for datacenter planning, three dimensional models are preferred.

IMPLEMENTATION GUIDANCE

- It is preferred to have vendor-supplied total system replacements able to ship out to the site within 24 hours via overnight shipment means.

3.3.12 HARDWARE MANAGEMENT SOFTWARE

STANDARD

ID	***Secondary Attribute***	***Specification***
12	Type	Agent or agent-less server management tool accessible through SNMP

	Automated Notification	Hardware events including exceptions, diagnostics, and failures, shall be exposed through SNMP with documented MIBs
	Shared Repository	Allows uploading all information collected by the tool into shared repository using ODBC or JBDC in a manner that preserves data fields for the diagnostic information (e.g., date/time, error code, module, description, system identification, status, system configuration)
	Support Level	Support level of management software must match support level of server hardware

EXPLANATION OF STANDARD

The tool should allow management of the hardware through a variety of means that interface with SNMP, and must be fully documented with MIBs for all relevant data (hardware events). Integration with VA's Enterprise Exception Log Service (EELS) is a consideration and is enabled through SNMP interfacing.

Ability to access event logs through database connectivity (JDBC or ODBC) is needed for future Enterprise Management Framework tools. Service could be provided through BIOS feature, OS-level features, or other layered features, and must provide the MIB documentation for accessing the information.

EVALUATION FACTORS

- Ability to integrate with a variety of industry enterprise-level system management tools is beneficial.
- Inclusion of an enterprise-level component with shared repository and correlation analysis features is beneficial.
- Ability to provide management of agent-less systems is beneficial.

IMPLEMENTATION GUIDANCE

- Support for SNMPv3 is preferred.
- A solution design that provides secure connections outside the physical facility is preferred.
- Automated vendor notification of failure, or pre-failure activity, to initiate vendor remediation is preferred.

3.3.13 RACK INFRASTRUCTURE COMPATIBILITY

STANDARD

ID	*Secondary Attribute*	*Specification*
13	Rack Unit Measurement	Up to 4U for rack-mount servers; blade implementations will be evaluated on an individual basis.
	Rail Type	Tool-less square-hole sliding
	Cable Management	Side-reversible for non-blade solutions

EXPLANATION OF STANDARD

Rack Unit Measurement – For this class of server, occupying more than 4U (or more than two blade slots) should not be necessary; 1 slot in a half-height blade chassis is fairly equivalent to a 1U rack-mount and 1 slot in a full-height blade chassis is fairly equivalent to a 2U rack-mount. It is expected that this class of server will be a 4U rack mount or double slot full-height blade server.

Rail Type – server must have rail adapters if needed to fit the generic non-proprietary type of rack specified in this standard.

Rack infrastructure standards must match the data center equipment rack standards.

EVALUATION FACTORS

- Lower occupied rack space or blade slot (per workload) is beneficial

IMPLEMENTATION GUIDANCE

3.3.14 OPERATING SYSTEM

STANDARD

ID	***Secondary Attribute***	***Specification***
14	Type	Linux preferred based on federal requirement to utilize open source operating systems, Windows acceptable, all must VA approved operating systems and compatible with hardware.
	Version	Current target version of Linux or Windows per VA TRM
	Vendor-Installed	Depends on data center policy; default is factory-installed with default settings and most recent patch level
	Support Level / Term	Must match hardware service level; term is three years with two option years unless VA has a standing enterprise software support agreement pertinent OS.

EXPLANATION OF STANDARD

Type – Linux is preferred as the most “open” type of option, but Windows is also acceptable as an industry-wide supported option. If UNIX is required Solaris is the preferred UNIX product. Solaris is preferred due to the “open” features and high level of government security certification.

Version – Operating system build, distribution, and version must be listed in the VA TRM.

Vendor-Installed – Data center policy may require local installation of the operating system. If this is not the case, the operating system should be factory-installed and have the most recent patches applied.

Support Level / Term – The operating system support level must be consistent with the criticality of the server and match hardware service level; term is three years with two option years unless VA has a standing enterprise software support agreement pertinent OS.

EVALUATION FACTORS

- Hardware support for the latest version of OS is beneficial.
- Installation of VA-supplied image is beneficial.

IMPLEMENTATION GUIDANCE

- UNIX requires exception justification and Solaris is the preferred UNIX product.
- Preference is for the latest versions of the operating system that are certified for implementation on the VA production network and supported by the hosted applications. If earlier versions are required due to compatibility limitations, these limitations should be documented for justification.

3.3.15 PLATFORM SOFTWARE / LICENSE

STANDARD

ID	***Secondary Attribute***	***Specification***
15	Multipath	Provides automated load balancing (all paths active) and fail-over; compatible with target storage array
	Data Backup	(optional) Matches requirements of the deployment location data center and SAN backup solution
	Monitoring Tool	Matches requirements of the deployment location data center
	Layered Framework	Defined by the application owner – meet license requirements for this server
	Server Management Tools	Matches requirements of the deployment location data center
	Availability / Recovery Tools	Matches the requirements for Persistent Computing standards applied to the hosted applications/services
	Security Tools	Follows Office of Information and Technology standards including compliance with FIPS, FISMA, and VA Directives.
	Virtual Management Software	For virtual environments, an Enterprise management tool is required

EXPLANATION OF STANDARD

Multipath – Require failover capability with all paths active; Include requisite multipath software from appropriate storage vendor to provide failover and load-balancing capabilities.

Data Backup – Although this type of server primarily uses backup tools for server image backup, there may (optionally) be a need for data backup tools. A data backup tool/agent might be required by some hosted applications that have local database storage. In addition, some applications might have data stored on the SAN and is covered by the SAN backup solution that requires an agent on the server. For these servers, enterprise data backup tools are being evaluated and might lead to an enterprise standard. In the meantime, the tool selection is driven by each data center location, and must adhere to security/encryption policies. This software is installed and configured by VA and might utilize existing/enterprise licenses.

Monitoring Tool and Server Management Tool – These are the agents required by server monitoring & management tools or other monitoring tools – if agents are required. It is expected that these tools will largely be defined by the Enterprise Management Framework. The tools must meet the VA EMF standards/tools, or be able to feed information directly into the EMF tools. Until such standards are available, these tools must meet the data center standards where the tools are being placed. This software is installed and configured by VA and might utilize existing/enterprise licenses.

Availability / Recovery Tools – These include agents or other software for image backup and restoration tools, service replication tools, and fail-over tools. These will be defined in the Persistent Computing standards and by the hosted application's model for persistent computing. This software might be installed/configured through a service contract associated with the server purchase, or might be installed/configured by VA.

Security Tools – must follow Office of Information and Technology standards including compliance with FIPS, FISMA, and VA Directives, and be implemented in a way that meets Certification and Accreditation (C&A) requirements. VA Enterprise Security Solution Service (ESSS) can provide a review of proposed security tools and can be reached by contacting the Enterprise Solutions Security Service under OI&T Field Security Operations.

Virtual Management Software – Virtual infrastructure requires and enterprise level management tool which may require additional licenses for each server. Live host migration may require specific network configurations or compliance with datacenter standards. Refer to LAN Standards, Section xx and Datacenter Standards, Section xx.

EVALUATION FACTORS

- Multipath – compatibility with a wide range of storage arrays / manufacturers is a benefit.

IMPLEMENTATION GUIDANCE

3.3.16 DATACENTER MANAGEMENT

STANDARD

ID	***Secondary Attribute***	***Specification***
16	Remote Keyboard/Video/Mouse Control	Ability to remotely connect to the server's external keyboard, video, and mouse ports through a networked KVM switch.

	Remote Power Disconnect	Ability to remotely disconnect/reconnect server to power source

EXPLANATION OF STANDARD

Remote Keyboard/Video/Mouse Control – A dongle to attach the server to a networked KVM switch is required. Refer to the Datacenter Standard, Section xx

Remote Power Disconnect – Ability to remotely disconnect/reconnect power source to server through the control of individual receptacles. Refer to Datacenter Standards, Section xx.

EVALUATION FACTORS

- Ability to remotely update device firmware is beneficial.
- Accessibility via web browser is beneficial – should support Microsoft Internet Explorer.

IMPLEMENTATION GUIDANCE

3.4 VISTA BACK-END (BE) (**CLASS E**)

The VistA Back-End (BE) server will provide all Caché database data access (via SAN based storage), with data servicing to Front-End (FE) servers over redundant private network paths. The BE servers will support 1-2 Vista database Server configurations, as well as VistA taskman operations. The BE server will also host the operating system based synchronous data replication, to facilitate the High Availability requirements of the metro-based platform. The metro-based platform will consist of clustered systems to further facilitate the High Availability survivability of the overall BE Regional platform.

The provided synchronous data replication, with server clustering, for the BE servers will initially be based on the OpenVMS based operating system from HP. The OpenVMS operating system, with clustering, and in many cases shadowing, have been supporting the VistA platform since the 1990's, and is also currently deployed in the existing RDP environment for both Region 1 and Region 4. This proven operating environment will continue for the BE servers to be deployed for Regions 2 & 3 VistA consolidation.

The BE servers may also include a "quorum" node. Cluster quorum configuration options include:

- Quorum processing site
- Quorum only site (first recommendation)
- Quorum cage (second recommendation)
- Primary datacenter (second recommendation)
- Primary side, floating between datacenters

A third computer room hosting the quorum node is the preferred and recommended configuration, in order to fully support automatic High Availability failover. The secondary recommendation is to host the quorum node at one of the two metro datacenters (per region), meaning, one of the two metro datacenters will be selected as the preferred (or primary), most

survivable datacenter. As such, this datacenter will house the quorum node, meaning the VMS cluster will only survive (without manual intervention) in this datacenter, in the event of an inter-site network link failure or a datacenter failure (by definition, the only datacenter which could fail and processing continue would be the secondary datacenter).

Quorum participation can be provided by:

- Quorum node (recommended)
- Quorum disk

The Quorum node is the preferred and recommended quorum participation method. This means an additional node, of minimal configuration, will be hosted at the primary datacenter location. This node will provide the vote tie-breaking mechanism, in the event there is an inter-site network link issue.

(add text on primary recommendation sizing)

Accepting the secondary recommendation (hosting quorum at the Primary datacenter), the quorum node is then proposed to be configured as a normal BE server, but to be used for Backup processing (the processing of nightly data backups) and as an online spare in the event of longer term node outages.

3.4.1 PROCESSOR

STANDARD

ID	*Secondary Attribute*	*Specification*
1	Type	IA_64 (Itanium)
	Socket Count	Minimum required to meet Performance Benchmark standard
	Core Count	Amount required to meet Performance Benchmark standard
	Cache	Minimum required to meet Performance Benchmark standard
	Virtualization Aware	Not Required

EXPLANATION OF STANDARD

Type – The current back-end architecture is built on, and only certified on the OpenVMS operating system. OpenVMS is supported on AlphaServer and Itanium (IA_64) based systems, and Alpha based servers are no longer available.

Socket Count – OpenVMS licensing is based on core-count. Socket Count should be the minimum required to satisfy the Performance Benchmark, with the assumption that core counts will increase with future generations of supported chip types.

Core Count – minimum amount expected for performance/capacity level is dual-core, more can be better. However, any amount that meets the Performance Benchmark specification is sufficient.

Cache – Minimum required to meet Performance Benchmark standard

Virtualization Aware – Not Required

EVALUATION FACTORS

- Currency of processor – most recent speed of processor is beneficial.

IMPLEMENTATION GUIDANCE

3.4.2 PERFORMANCE

STANDARD

ID	*Secondary Attribute*	*Specification*
2	Performance Benchmark	SPEC CPU2006 Integer Rate Base value >= 90

EXPLANATION OF STANDARD

This SPEC_Int rate is represented by a large number of server platforms. Performance requirement is largely dependent on the application's workload and compute-resource consumption profile. For example, the Cleveland VAMC is considered a very large VistA environment, and has been piloting the Itanium based server Front End. The daily average M Command utilization for Cleveland is reported to be 800,000 to 900,000. These levels consume the older ES80 model 8 (8 CPUs), and utilize about 1/3 to ½ of an Itanium based server (for the daily average). Other data suggests Itanium based servers are more than twice as powerful as Alpha based servers, with similar core or CPU counts (as appropriate for the technology). Considering the peak period requirements, and allowing for performance spikes, as well as the failover and switchover requirements will generally double the capacity requirements of the BE severs, implementing servers twice as capable as the currently deployed alpha platform is appropriate. The SPEC2000 value for deployed ES80 systems is 62 or 73 (depending on chip speed). The SPECint_rate2006 (published Nov 2006) value for rx6600/BL870c (Itanium based) servers is 91.1. It is assumed the Spec2006 performance mtric is more difficult, and returns lowers values, as compared with SPEC2000 ratings. For this exercise, it is assumed SPEC2006 values would be about ½ what they might have been if measured under SPEC2000 (i.e. the rx6600 SPEC2006 value of 91.1 might have had a SPEC2000 value near 180).

EVALUATION FACTORS

- Higher benchmark rating value is beneficial.

IMPLEMENTATION GUIDANCE

3.4.3 MEMORY

STANDARD

ID	Secondary Attribute	Specification
3	Type	Compatible with CPU with full error correction capability including ECC
	Total Memory	Minimum 24GB usable
	Speed	Minimum - match operational CPU and bus speed required to meet the Performance Benchmark requirement

EXPLANATION OF STANDARD

Type – Memory has to be highly reliable – ECC is the expected feature to allow higher levels of reliability. RDIMM is more expandable/scalable and provides additional reliability features (e.g., more error-checking features) while consuming more power (about one watt per chip) and costing more. In general, RDIMM is recommended with high memory requirements and higher availability requirements.

Total Memory – Itanium memory usage expected to be about 20% greater than existing alpha-based system. InterSystems' recommendation also calls for 3-5 MB per process, in terms of global buffer sizing.

Using 16 GB for a base server, with 8 cores, and adding 2.5 GB (based on 500 Taskman jobs with 5MB buffer space per process) for global buffer cache, with any server possibly supporting up to 3 configurations (in a failover or switchover situation), this sizing accounts for 16 GB for typical server processing (Db serving, Taskman processes, general overhead) plus 7.5 GB for Caché global buffers.

Speed – Memory speed is expected to be matched by the vendor, to match processor capabilities. As Itanium servers are expected to be only available from HP, vendor dependence is warranted.

EVALUATION FACTORS

- Additional memory is beneficial
- Higher density chips while avoiding a decrease in memory bus speed is preferred.
- Speed of memory takes precedence over density as long as capacity is met

IMPLEMENTATION GUIDANCE

- RDIMM is recommended for high memory requirements and higher availability requirements.

3.4.4 INTERNAL STORAGE

STANDARD

ID	Secondary Attribute	Specification

4	Type	SAS
	Quantity of Drives	Minimum one (DOSD – i.e. to host Dump Off System Disk)
	RAID Configuration	Not Required
	Drive Speed	Minimum 10K RPM
	Drive Capacity	Minimum 36GB usable storage capacity
	Disk Subsystem Performance	The disk must meet or exceed the performance levels specified below for tests "Transaction Rate" and "Throughput Rate" Validation will be incorporated in user acceptance phase.
	Controller Cache	Not Required
	Quantity of Controllers	Minimum of one

EXPLANATION OF STANDARD

Type – SAS is required for the following reasons: 1) SAS uses the SCSI command set which provides better error reporting and recovery techniques than does SATA, 2) SATA throughput can be degraded on SAS adapters that use the Serial Tunneling Protocol (STP) to communicate with SATA targets, and 3) because they are engineered for continuous duty cycles and longer MTBFs, SAS drives are an accepted industry standard for enterprise server solutions.

Quantity – The Backend servers will SAN boot, and otherwise access all required data from the SAN. However, a local disk for possible booting, or more likely hosting the creation of system crash memory dumps will be useful. A local disk may be required for this function.

RAID Configuration – An internal disk could serve as a host to operating system dumps generated thru a system crash. The longer term retention of these files is also considered. Assuming dump files of 10 GB in size (or less), the desire is to retain at least 3 copies of recent crash dumps. An internal system disk is not expected to be required.

Drive Speed – Minimum RPM for this class of server & storage is 10K..

Drive Capacity – 36GB minimum usable storage capacity is sufficient for the dump file, and optional older dump file disk storage needs.

Disk Subsystem Performance – The disk must meet or exceed the performance levels specified below for tests "Transaction Rate" and "Throughput Rate" as described in APPENDIX G.

- Transaction Rate = 500+ IOPS
- Throughput Rate = 50+ MBPS

Controller Cache – Cache is not required because disk subsystem will only be used to store dump files.

Quantity of Controllers – Only one SAS controller is required.

EVALUATION FACTORS

- Higher storage capacity is beneficial
- Higher RPM is beneficial for drive platters
- Additional internal drives is beneficial

IMPLEMENTATION GUIDANCE

3.4.5 EXTERNAL STORAGE INTERFACE

STANDARD

ID	***Secondary Attribute***	***Specification***
5	Type	Fiber-channel with duplex LC connectors
	Port Count	Minimum of four ports with full port redundancy provided.
	Bandwidth	Minimum 4Gbps; must meet or exceed SAN fabric requirements
	Compatibility	Support storage arrays at deployment location; supported by operating system and multipath drivers specified for this server
	SAN Boot Capability	BIOS support for SAN boot
	Blade Chassis Component (if applicable)	Pass thru connections, for increased bandwidth capabilities
	Hardware Redundancy	Supports connecting redundant ports configured to separate switches on the SAN. Minimum redundant ports

EXPLANATION OF STANDARD

- Type – fiber channel and Ethernet are the vast majority of investment for connections used in storage-dedicated networks in VA data centers, and exceptions should be justified including impact to existing infrastructure investment. Typical Ethernet connector types are RJ-45 for copper and LC for optical. When Ethernet is used, TCP Offload Engine (TOE) is preferred for all servers. Drivers are more readily available for Windows than Linux servers.
- Port Count – minimum required for port-level redundancy / load-balancing. Provides the flexibility to improve the throughput and performance without further hardware changes. Can initially configure with only 2 active.

Potential benefit for separating the ports used for booting and data. Allows increased workload of multiple database servers in shared server environment.

- Bandwidth – 4Gbps is standard for current investment of optical fabrics in the storage systems and infrastructure in VA data centers and matches the minimum current industry standard; similarly 1Gbps is standard for current investments and minimum current industry practices when using copper-based storage fabrics.
- Compatibility – Support storage subsystems at deployment locations. Check adapter compatibility for storage at deployment location. Don't want to provide a list of brand names.
- Blade Chassis Components – Considering the bandwidth requirements of network connections (Ethernet and SAN), pass-thru connections preferred at this time.
- Hardware Redundancy – All storage communication connections should provide full redundancy, from the option card, port, and switch connectivity.

EVALUATION FACTORS

- For a server with high criticality of SAN storage connectivity, redundant adapter cards are recommended.
- Interface for iSCSI can be termed an HBA interface or a NIC interface. Where higher performance is a concern, the HBA interface is recommended.

IMPLEMENTATION GUIDANCE

- For a server with high criticality of SAN storage connectivity, redundant adapter cards are recommended.
- Interface for iSCSI can be termed an HBA interface or a NIC interface. Where higher performance is a concern, the HBA interface is recommended.
- Bandwidth spread across multiple ports on independent cards may be required for performance reasons
- Backend Server for VistA require daily disk to disk backups of both synchronous copies of production databases as well as for both copies of the CSJ provided databases (between regions). Further, at least one copy of each database (production and CSJ) must be archived for later restoration if needed. The Production and CSJ database backups strategy should be documented in the SAN/Storage/Back-up standards document.

3.4.6 SERVER COMMUNICATIONS INTERFACE

STANDARD

ID	***Secondary Attribute***	***Specification***
6	Type	Ethernet matching connector type for network in data center
	Port Count	Minimum of 6 ports
	Bandwidth	Minimum 1Gbps
	Hardware Redundancy	Supports connecting redundant ports configured to separate switches on the LAN; supports physically independent redundant ports including embedded ports for each interface function (e.g., public network function and cluster interconnect function)

	Blade Chassis Component (if applicable)	Pass Thru connections

EXPLANATION OF STANDARD

Type – Ethernet is the vast majority of investment for connections used in data center networks in VA, and exceptions should be justified including impact to existing infrastructure investment. Typical Ethernet connector types are RJ-45 for copper and LC for optical with a future trend towards copper only.

Port Count – when used in a virtual environment, a base set of 4 ports are used for virtual guests, 1 is for the console, and 1 for the live migration. Other specific interfaces may be required depending on the profile of the workload/application. When not used in a virtual environment, cluster interconnects may need 2 or more ports, depending on the amount of cluster traffic (e.g., Oracle clusters send data over the cluster interconnect, simple Microsoft clustering only send "heartbeat" traffic).

Bandwidth – expected standard interface on network switches is 1Gbps. There is a potential for 10Gbps Ethernet.

Hardware Redundancy – embedded ports count as one "card"; all interface uses are spread across two "cards" (including at least one add-on NIC). The goal is physical separation of the chipset/ASIC used on the redundant port, for each function. Support for "simple failover" (with a single IP address) and independent usage (with multiple IP addresses) is required.

Blade Chassis Component – Due to the small form factor of the blade chassis, pass thru connections are required.

EVALUATION FACTORS

- Additional cards can be beneficial
- Support for active/active load balancing is beneficial

IMPLEMENTATION GUIDANCE

- Backend Server for VistA requires ECP (Caché Enterprise cache Protocol) communication between the Backend DB servers, and Frontend Application Servers. This ECP communication must support the spanning of metro-datacenters, without changing the underlying IP address, as defiend by the Application Server connection to the DB server. The Production ECP communication strategy should be documented in the LAN standards document (see GSS/ACE discussion).

- Backend Server for VistA requires SCS (VMScluster System Communications Services) communication between each cluster member in both (all) metro-datacenters. The SCS protocol cannot be routed, and thus must be bridged. The Production SCS communications strategy should be documented in the LAN standards document (see SCS ACE or layer 2 tunneling discussion).

3.4.7 REMOVABLE MEDIA DEVICE

STANDARD

ID	Secondary Attribute	Specification
7	Optical Drive	CD/DVD drive – minimum 24x speed
	USB	Not Required

EXPLANATION OF STANDARD

The functional requirement supported by this standard is to provide a media transfer mechanism to upload patch and software/firmware installation, upload diagnostic tools, and (with read/write capability) to download diagnostic information. Manufacturers are going toward a trend of using USB flash drives for sending patch/upgrade/firmware distributions. Therefore, the requirement is to provide both CD/DVD and USB flash drive capabilities. Note that security restrictions or concerns need to be addressed before using removable media.

The type of drive specified is the typical expected minimum specification and type.

Alternative Removal Media Device access must be quoted and provided in cases where an internal device of this type is not configured or available.

EVALUATION FACTORS

- Having a DVD drive is beneficial.
- Faster speeds and/or Read-write capability is beneficial (additional security checks may be required for read/write capability).

IMPLEMENTATION GUIDANCE

- Preferred to provide removable media device for patch and software installation options; but small form factor (e.g., blade) servers might use other options. Media access type must be provided for, as configured by vendor.

3.4.8 POWER

STANDARD

ID	Secondary Attribute	Specification
8	Redundancy	N+1 redundancy on power supply
	Voltage	208V input voltage on power supply
	Cord Type	IEC

	Power Efficiency	Until such time that there are Energy Star ratings available to most server classes, power efficiency should be consistent with industry trends.
	Power Consumption Documentation	Vendor-supplied data for power consumption of specified configuration at 100% load, "typical" active usage, and at idle.

EXPLANATION OF STANDARD

Redundancy – server must continue to operate if and when a power supply fails in order to enhance availability.

Voltage and cord type – driven by data center standards, 208V can more efficiently use power from utility

Power Efficiency – Certifications for power efficiency include: 80-plus (Dell & HP certify through them, but IBM does not), and Energy Star (still forming the standard for servers, but blade servers will be separate standard). The EPA establishes Energy Star standards – tier 2 appears to be the four-socket type of server while tier 1 appears to be the dual-socket server types. Some server manufacturers implement power efficiency management features including step-down of power consumption during low resource-consumption states.

Power Consumption Documentation – Preferred documentation is Energy Star data sheet and/or SPECpower_ssj2008 published results.

EVALUATION FACTORS

- Power management/economy and reporting/analysis features are beneficial.
- Lower power consumption rating at 100% utilization per workload capacity (in terms of SPECint_rate value) is beneficial.

IMPLEMENTATION GUIDANCE

- Cord type of IEC-C13 is preferred for most classes of rack-mount servers

3.4.9 COOLING FAN

STANDARD

ID	***Secondary Attribute***	***Specification***
9	Redundancy	Minimum N+1 redundancy

EXPLANATION OF STANDARD

Redundancy – server must continue to operate if and when a fan fails in order to enhance availability.

EVALUATION FACTORS

- Additional fans or separation of fans into multiple cooling zones is beneficial.
- Lower total decibel rating on the fans is beneficial.

IMPLEMENTATION GUIDANCE

3.4.10 OUT OF BAND MANAGEMENT

STANDARD

ID	Secondary Attribute	Specification
10	Type	Remote command-line and console-level access utilizing dedicated network interface
	Security	Secure IP-based remote management that complies with all VA security requirements
	Remote Power Control	Ability to remotely power on/off/reset server

EXPLANATION OF STANDARD

Required dedicated network interface is required outside of the other network interfaces specified in section 3.2.7.

Based on data center environment, operational needs, and minimum requirements that are typically satisfied through a wide variety of servers. Includes access for diagnostic capability.

Remote Power Control – Ability to power on/off/reset through server based management.

Console logging – OpenVMS generates OPCOM (Operator Communications) messages related to operating system related actions and possible error conditions. This information can be invaluable after an event, as part of troubleshooting. It is required that a solution be offered to log all OPCOM messages from the console, for historical purposes.

EVALUATION FACTORS

- Ability to remotely mount a drive or ISO is beneficial. This can be used for software, firmware and OS updates using remote drive mounting, and it minimizes the need for local optical drive.
- Active Directory integration for authentication is beneficial.
- Role-based access control is beneficial.
- Accounting capability is beneficial.
- Strong password compliance is beneficial.
- Accessibility via web browser is beneficial – should support Microsoft Internet Explorer.
- Support for Secure Shell (SSH) connections is beneficial – should be FIPS 140-2 compliant.
- Ability to remotely identify server with visual indicator (e.g., indicator light) is beneficial.

IMPLEMENTATION GUIDANCE

3.4.11 SERVER HARDWARE VENDOR SUPPORT

STANDARD

ID	Secondary Attribute	Specification
11	Type	Match service level requirement for hosted applications; mission-critical level support shall include 24x7 coverage 365 days/year, less than 1 hour initial engineer-level response time, 4-hour on-site response time for emergency dispatches, and 8-hour time-to-repair
	Term Length	Minimum of three years with two additional option years
	Keep Your Hard Drive	All storage drives are kept by VA in the event of warranty/service replacement

EXPLANATION OF STANDARD

Type – the level of support matches the criticality level of the hosted services. Mission-critical level is defined in this standard, and has been shown to be accommodated by major server vendors. Other levels will have to be defined to match the business expectations of that criticality level. A non-critical example would be 8 business hours/weekday phone coverage with next-day response and repair. Access to original server manufacturer support with the option to escalate to senior technicians at VA discretion is required.

Term – some components might only allow three years of support on an initial contract, but option years must be available to extend that to the expected lifetime of the system which is nominally five years.

Keep Your Hard Drive – This is a security requirement that is now a de-facto standard in VA.

EVALUATION FACTORS

- Lower on-site response time is beneficial.
- Lower initial “engineer level” contact response time is beneficial.
- Lower time-to-repair is beneficial.
- Vendor-supplied components stocked as spares near, or at, facility is beneficial.
- Penalty clauses for vendor not meeting support contract provides benefit.
- Allowance for optional parts-delivery/customer-installation of hot swappable components, memory, and drop-in cards beneficial at the VA’s option.
- Access to electronic models of equipment being proposed is beneficial. Because electronic models will be used with CAD and visual design applications for datacenter planning, three dimensional models are preferred.

IMPLEMENTATION GUIDANCE

- It is preferred to have vendor-supplied total system replacements able to ship out to the site within 24 hours via overnight shipment means.

3.4.12 HARDWARE MANAGEMENT SOFTWARE

STANDARD

ID	*Secondary Attribute*	*Specification*
12	Type	Agent or agent-less server management tool accessible through SNMP
	Automated Notification	Hardware events including exceptions, diagnostics, and failures, shall be exposed through SNMP with documented MIBs
	Shared Repository	Allows uploading all information collected by the tool into shared repository using ODBC or JBDC in a manner that preserves data fields for the diagnostic information (e.g., date/time, error code, module, description, system identification, status, system configuration)
	Support Level	Support level of management software must match support level of server hardware

EXPLANATION OF STANDARD

The tool should allow management of the hardware through a variety of means that interface with SNMP, and must be fully documented with MIBs for all relevant data (hardware events). Integration with VA's Enterprise Exception Log Service (EELS) is a consideration and is enabled through SNMP interfacing.

Ability to access event logs through database connectivity (JDBC or ODBC) is needed for future Enterprise Management Framework tools. Service could be provided through BIOS feature, OS-level features, or other layered features, and must provide the MIB documentation for accessing the information.

EVALUATION FACTORS

- Ability to integrate with a variety of industry enterprise-level system management tools is beneficial.
- Inclusion of an enterprise-level component with shared repository and correlation analysis features is beneficial.
- Ability to provide management of agent-less systems is beneficial.

IMPLEMENTATION GUIDANCE

- Support for SNMPv3 is preferred.
- A solution design that provides secure connections outside the physical facility is preferred.
- Automated vendor notification of failure, or pre-failure activity, to initiate vendor remediation is preferred.

3.4.13 RACK INFRASTRUCTURE COMPATIBILITY

STANDARD

ID	Secondary Attribute	Specification
13	Rack Unit Measurement	7U or 10U for rack-mount servers; 4-slot blade for blade servers
	Rail Type	Tool-less square-hole sliding
	Cable Management	Side-reversible for non-blade solutions

EXPLANATION OF STANDARD

- Rack Unit Measurement – For this class of server, occupying more than 10U (or four blade slots) should not be necessary
- Rack infrastructure standards must match the data center equipment rack standards.

EVALUATION FACTORS

- Lower occupied rack space or blade slot (per workload) is beneficial

IMPLEMENTATION GUIDANCE

3.4.14 OPERATING SYSTEM

STANDARD

ID	Secondary Attribute	Specification
14	Type	OpenVMS, Un-Limited User Licensing, VMS clustering, Host Based Volume Shadowing, TCP/IP Services
	Version	OpenVMS version 8.3 (minimum version support)
	Vendor-Installed	Not Required, but preferred
	Support Level / Term	Must match hardware service level; term is three years with two option years unless VA has a standing enterprise software support agreement pertinent OS.

EXPLANATION OF STANDARD

Type – OpenVMS based servers are the current and preferred operating system for Back End server to support the replication and availability requirements of the RDP consolidated environments.

Unlimited User licensing will offer the flexibility of supporting additional users as needed for automatic failover operations (when nodes or data centers fail) as well as switchover operations, when a regions entire metro-area cluster fails.

VMS clustering will facilitate and allow automatic node, configuration, and VistA failover, in the event of node failures or crashes. Clustering will also help facilitate failover if and when single data-centers fail or otherwise become unavailable for operations.

Host Based Volume Shadowing (HBVS) is the supported mechanism of OpenVMS to synchronously replicate data between metro-data centers assuring data survivability against metro data center failure or loss.

TCP/IP is the currently deployed TCP solution for OpenVMS, within the VA.Version – Operating system build, distribution, and version must be listed in the VA TRM.

Vendor-Installed – Not Required, but preferred

Support Level / Term – The operating system support level must be consistent with the criticality of the server and match hardware service level; term is three years with two option years unless VA has a standing enterprise software support agreement pertinent OS.

EVALUATION FACTORS

- Hardware support for the latest version of OS is beneficial.

IMPLEMENTATION GUIDANCE

3.4.15 PLATFORM SOFTWARE / LICENSE

STANDARD

ID	*Secondary Attribute*	*Specification*
15	Multipath	Provides automated load balancing (all paths active) and fail-over; compatible with target storage array
	Data Backup	(optional) Matches requirements of the deployment location data center and SAN backup solution
	Monitoring Tool	Matches requirements of the deployment location data center
	Layered Framework	Support for InterSystems' Caché (minimum version 5.2.3)
	Server Management Tools	Matches requirements of the deployment location data center
	Availability / Recovery Tools	Matches the requirements for Persistent Computing standards applied to the hosted applications/services

	Security Tools	Follows Office of Information and Technology standards including compliance with FIPS, FISMA, and VA Directives.
	Virtual Management Software	Not Required

EXPLANATION OF STANDARD

Multipath – Require failover capability with all paths active; Include requisite multipath software from appropriate storage vendor to provide failover and load-balancing capabilities.

Data Backup – Although this type of server primarily uses backup tools for server image backup, there may (optionally) be a need for data backup tools. A data backup tool/agent might be required by some hosted applications that have local database storage. In addition, some applications might have data stored on the SAN and is covered by the SAN backup solution that requires an agent on the server. For these servers, enterprise data backup tools are being evaluated and might lead to an enterprise standard. In the meantime, the tool selection is driven by each data center location, and must adhere to security/encryption policies. This software is installed and configured by VA and might utilize existing/enterprise licenses.

Monitoring Tool and Server Management Tool – These are the agents required by server monitoring & management tools or other monitoring tools – if agents are required. It is expected that these tools will largely be defined by the Enterprise Management Framework. The tools must meet the VA EMF standards/tools, or be able to feed information directly into the EMF tools. Until such standards are available, these tools must meet the data center standards where the tools are being placed. This software is installed and configured by VA and might utilize existing/enterprise licenses.

Layered Framework – The VistA application suite is built on InterSystems' Caché, with the currently deployed version of 5.2.3.

Availability / Recovery Tools – These include agents or other software for image backup and restoration tools, service replication tools, and fail-over tools. These will be defined in the Persistent Computing standards and by the hosted application's model for persistent computing. This software might be installed/configured through a service contract associated with the server purchase, or might be installed/configured by VA.

Security Tools – must follow Office of Information and Technology standards including compliance with FIPS, FISMA, and VA Directives, and be implemented in a way that meets Certification and Accreditation (C&A) requirements. VA Enterprise Security Solution Service (ESSS) can provide a review of proposed security tools and can be reached by contacting the Enterprise Solutions Security Service under OI&T Field Security Operations.

Virtual Management Software – Virtual infrastructure requires and enterprise level management tool which may require additional licenses for each server. Live host migration may require specific network configurations or compliance with datacenter standards. Refer to LAN Standards, Section xx and Datacenter Standards, Section xx.

EVALUATION FACTORS

- Multipath – compatibility with a wide range of storage arrays / manufacturers is a benefit.

IMPLEMENTATION GUIDANCE

3.4.16 DATACENTER MANAGEMENT

STANDARD

ID	*Secondary Attribute*	*Specification*
16	Remote Keyboard/Video/Mouse Control	Ability to remotely connect to the server's external keyboard, video, and mouse ports through a networked KVM switch.
	Remote Power Disconnect	Ability to remotely disconnect/reconnect server to power source

EXPLANATION OF STANDARD

Remote Keyboard/Video/Mouse Control – A dongle to attach the server to a networked KVM switch is required. Refer to the Datacenter Standard, Section xx

Remote Power Disconnect – Ability to remotely disconnect/reconnect power source to server through the control of individual receptacles. Refer to Datacenter Standards, Section xx.

EVALUATION FACTORS

- Ability to remotely update device firmware is beneficial.
- Accessibility via web browser is beneficial – should support Microsoft Internet Explorer.

IMPLEMENTATION GUIDANCE

4 TAXONOMY OF STANDARDS

[Build taxonomy of this standard, defining the primary and secondary attributes common to all standards sets that will be contained in this standard. Add additional rows and cells as necessary. This attribute set will be used to populate the tables in Sections 2 and 3. Replace this paragraph with a paragraph introducing your taxonomy.]

ID	*Primary Attribute*	*Secondary Attribute*
1	Processor	Type

ID	*Primary Attribute*	*Secondary Attribute*
		Socket Count
		Core Count
		Cache
		Virtualization Aware
2	Performance	Performance Benchmark
3	Memory	Type
		Total Memory
		Speed
4	Internal Storage	Type
		Quantity of Drives
		RAID Configuration
		Drive Speed
		Drive Capacity
		Disk Subsystem Performance
		Controller Cache
		Quantity of Controllers
5	External Storage Interface	Type
		Port Count
		Bandwidth
		Compatibility
		SAN Boot Capability
		Blade Chassis Component (if applicable)
		Hardware Redundancy
6	Server Communications Interface	Type
		Port Count
		Bandwidth
		Hardware Redundancy
		Blade Chassis Component (if applicable)
7	Removable Media Device	Optical Drive

ID	*Primary Attribute*	*Secondary Attribute*
		USB
8	Power	Redundancy
		Voltage
		Cord Type
		Power Efficiency
		Power Consumption Documentation
9	Cooling Fan	Redundancy
10	Out of Band Management	Type
		Security
		Remote Power Control
11	Server Hardware Vendor Support	Type
		Term Length
		Keep Your Hard Drive
12	Hardware Management Software	Type
		Automated Notification
		Shared Repository
		Support Level
13	Rack Infrastructure Compatibility	Rack Unit Measurement
		Rail Type
		Cable Management
14	Operating System	Type
		Version
		Vendor-Installed
		Support Level / Term
15	Platform Software / License	Multipath
		Data Backup
		Monitoring Tool

ID	*Primary Attribute*	*Secondary Attribute*
		Layered Framework
		Server Management Tools
		Availability / Recovery Tools
		Security Tools
		Virtual Management Software
16	Datacenter Management	Remote Keyboard/Video/Mouse Control
		Remote Power Disconnect

APPENDIX A – DEFINITIONS

- **Mission-Critical** - One description of mission-critical criticality level for system platforms is provided below for reference:

  Mission Critical Information
  - Business Value: Essential to fundamental business operations – outage seriously impairs functioning of business
  - Outage Impact: Interruption of service may result in severe financial, regulatory, safety, patient health, or other business issues
  - Significant Outage: More than five minutes of downtime is considered significant at any time

- **Cache** - Small memories on or close to the CPU that can speed up processing by reducing the number of times a CPU has to access much slower main memory. All CPUs have level 1 (L1) cache and may also have level 2 (L2) and level 3 (L3) cache.

- **SPEC CPU2006 Integer Rate Base** - CPU2006 is a set of benchmarks designed to test the CPU performance of a server computer system. This benchmark is usually run on only a single CPU (even if the system has many CPUs) and only on a single core if the CPU has multiple cores. The "SPEC CPU2006 Integer Rate Base" is a more complete system-level benchmark that allows all CPUs to be used.

- **N+1** - Need plus one, a redundancy concept where capacity is configured to include planned capacity plus one additional device to enable continued operations with the failure of one system in the configuration. This presumes immediate detection and remediation of the failed unit.

- ***n*U (or Rack Unit)**- A rack unit or U is a unit of measure used to describe the height of equipment intended for mounting in a 19-inch rack. The size of a piece of rack mounted equipment is frequently described as a number in "U". For example, one rack unit is often referred to as "1U", 2 rack units as "2U" and so on.

- **SAS (Serial Attached SCSI)** - A data-transfer technology that moves data to and from computer storage devices such as hard drives and tape drives.

- **ECC (Error-Correcting Code)** - Due to electrical or magnetic interference inside a computer system, single bits of memory can spontaneously flip to the opposite state. To mitigate this, ECC enabled memory detect single-bit errors and correct them.

- **CPU (Central Processing Unit)** - The Central Processing Unit (CPU) or processor is the portion of a computer system that carries out the instructions of a computer program, and is the primary element carrying out the computer's functions.

- **x86_64** - In CPU design, x86-64 is an extension of the x86 instruction set. It allows far larger virtual and physical address spaces than x86_32 designs, doubles the width of the integer registers from 32 to 64 bits, increases the number of integer registers, and provides other enhancements. It is also known as x64.

APPENDIX B – REFERENCES

SPEC http://www.spec.org/

Serial ATA International http://www.serialata.org/index.asp

Oracle Weblogic http://www.oracle.com/appserver/weblogic/weblogic-suite.html

VA LAN Standards [place URL link here]

VA WAN Standards [place URL link here]

VA Datacenter Standards [place URL link here]

VA Storage Standards [place URL link here]

APPENDIX C – ACRONYMS

Refer to the VA Acronym Lookup Web page for a list of VA specific acronyms.

NIC	Network Interface Controller
HBA	Host Bus Adapter
DDR2	Double Data Rate 2 (a Memory interface specification)
AMD	Advanced Micro Devices, Inc.
SPEC	Standard Performance Evaluation Corporation
ECC	Error-Correcting Code
MB	Megabytes
Mbps	Megabits per Second
GB	Gigabytes
Gbps	Gigabits per Second
RPM	Rotations per Minute
IEC	International Electrotechnical Commission
GHz	Gigahertz
SAS	Serial Attached SCSI
PCI-E	PCI-Express (or Peripheral Component Interconnect Express)
RDIMM	Registered Dual In-line Memory Module
ASIC	Application-Specific Integrated Circuit
LC	Lucent Connector (or Local Connector)
BIOS	Basic Input/Output System
IOPS	Input/Output Operations Per Second

APPENDIX D – CONTRIBUTORS

Michael Julian	Data center Design
Michael Bell	Information Modeling
David Deaderick	Linux/Oracle/WebLogic Server Hardware
John Beaufait	
David Carter	
Nelda Cook	
John Mehl	
Robert Moser	
Franco Susi	
Kurt Virnig	
James Yaple	
David Wong	
Mark Zimmerman	
Denise McLain	
John Dellar	
Jeff Lawlor	

APPENDIX F – SERVER CLASSES

The following list of common server functions associates function and workload with particular server classes. This list is not intended to be all inclusive but simply a starting point or guide on how to map server function and workload with a server class.

The following table provides a mapping of server functions to server classes:

Server Function	Standard Class for LIGHT Workload	Standard Class for TYPICAL Workload	Standard Class for HEAVY Workload
AudioCare	CLASS C[1]	CLASS C[1]	CLASS C[1]
Domain Controller	CLASS C[7]	CLASS B	CLASS B
Data Backup	CLASS B	CLASS B	CLASS B
File server	CLASS C	CLASS B	CLASS B
Print server	CLASS C	CLASS C	CLASS C
Web or FTP server	CLASS C	CLASS C	CLASS C
Database	CLASS B	CLASS B	CLASS A
Exchange	N/A	CLASS A[4]	CLASS A[4]
Management Application (e.g. ePO, Ciscoworks, Orion, etc)	CLASS B[5]	CLASS A[5]	CLASS A[5]
Management Application w/o database (SAN management app – e.g. HP Commandview)	CLASS C	CLASS B	CLASS B
Application server (e.g. Weblogic JVM)	CLASS C	CLASS B	CLASS B
SCCM Application	N/A	CLASS B	CLASS A
SCCM Database	N/A	CLASS B	CLASS A
SCCM Delivery	N/A	CLASS C[8]	CLASS B
SharePoint MOSS	N/A	CLASS B	CLASS A
Terminal Server	CLASS C	CLASS B	CLASS B
Virtual Host	CLASS B[6]	CLASS A	CLASS A
VistA Front-end Application	CLASS C[3]	CLASS C[3]	CLASS C[3]
VistA Imaging Background Processor	CLASS B[2]	CLASS B[2]	CLASS B[2]
VistA Imaging Gateway	CLASS C	CLASS C	CLASS C
WSUS (update servers)	CLASS C	CLASS B	CLASS B
VistA Back-end server	N/A	CLASS E	CLASS E

1. Class C with potential need for form factor exemption
2. Class B due to clustering and SAN activity
3. Quantity dependent (used in a scale-out model)
4. Class A with application specific modifications
5. Class A or B; workload will vary depending upon whether it is dedicated or shared
6. Used to host one or two virtual guests for high availability only
7. Read-Only domain controller
8. May require external storage

APPENDIX G – DISK SUBSYSTEM PERFORMANCE TEST

The tests described in this section use IOMeter version 2006.07.27 to evaluate the performance of a server's disk subsystem. There are two tests described; the "Transfer Rate" test which is measured in I/O operations per second (IOPS) and the "Throughput Rate" test which is measured in megabytes per second (MBPS).

Before the tests can be run, IOMeter must be setup with a baseline configuration. This can be achieved by copying the contents of TABLE 1 into a file, saving the file with a .icf extension, and opening it with IOMeter. The final step in configuring IOMeter is setting the queue depth to 4. On the first screen when IOMeter is started, there is a parameter named "*# of Outstanding I/O's*". Change this parameter from 1 to 4.

Once IOMeter has been configured, perform the following:

1. Select "*Worker 1*" in the left pane.
2. Select the "*Disk Targets*" tab then select the disk to be tested.
3. Select the "*Access Specifications*" tab then select the "*4K 67% Read – Random*" test in the left pane and the "*Add*" button.
4. Select the "*Start Tests*" button (the green flag on the top toolbar). When asked for a file name, use the default value of "*results*".
5. Let the test run until it stops (5 minutes)

The results are located in the "results.csv" file create before the test. Opening the file in Excel, the test results can be found:

TEST 1: TRANSACTION RATE – Column G under "IOps"

TEST 2: THROUGHPUT RATE – Column J under "MBps"

TABLE 1: IOMETER CONFIGURATION FILE

```
Version 2006.07.27
'TEST SETUP ====================================================================
'Test Description

'Run Time
'                hours      minutes    seconds
                 0          5          0
'Ramp Up Time (s)
                 0
```

```
'Default Disk Workers to Spawn
                NUMBER_OF_CPUS
'Default Network Workers to Spawn
                0
'Record Results
                ALL
'Worker Cycling
'               start      step       step type
                1          1          LINEAR
'Disk Cycling
'               start      step       step type
                1          1          LINEAR
'Queue Depth Cycling
'               start      end        step       step type
                1          32         2          EXPONENTIAL
'Test Type
                NORMAL
'END test setup
'RESULTS DISPLAY ==============================================================
'Update Frequency,Update Type
                0,WHOLE_TEST
'Bar chart 1 statistic
                Total I/Os per Second
'Bar chart 2 statistic
                Total MBs per Second
'Bar chart 3 statistic
                Average I/O Response Time (ms)
'Bar chart 4 statistic
                Maximum I/O Response Time (ms)
'Bar chart 5 statistic
                % CPU Utilization (total)
'Bar chart 6 statistic
                Total Error Count
'END results display
'ACCESS SPECIFICATIONS ========================================================
'Access specification name,default assignment
                Default,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                4096,100,67,100,0,1,0,0
'Access specification name,default assignment
                4K 67% Read - Random,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                4096,100,67,100,0,4,0,0
'Access specification name,default assignment
                4K 100% Read - Random,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                4096,100,100,100,0,4,0,0
'Access specification name,default assignment
                4K 0% Read - Random,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                4096,100,0,100,0,4,0,0
'Access specification name,default assignment
                4K 100% Read - Sequential,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                4096,100,100,0,0,4,0,0
'Access specification name,default assignment
                4K 0% Read - Sequential,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                4096,100,0,0,0,4,0,0
'Access specification name,default assignment
                32K 67% Read - Random,NONE
```

```
'size,% of size,% reads,% random,delay,burst,align,reply
                32768,100,67,100,0,4,0,0
'Access specification name,default assignment
                32K 100% Read - Random,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                32768,100,100,100,0,4,0,0
'Access specification name,default assignment
                32K 0% Read - Random,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                32768,100,0,100,0,4,0,0
'Access specification name,default assignment
                32K 100% Read - Sequential,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                32768,100,100,0,0,4,0,0
'Access specification name,default assignment
                32K 0% Read - Sequential,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                32768,100,0,0,0,4,0,0
'Access specification name,default assignment
                64K 67% Read - Random,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                65536,100,67,100,0,4,0,0
'Access specification name,default assignment
                64K 100% Read - Random,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                65536,100,100,100,0,4,0,0
'Access specification name,default assignment
                64K 0% Read - Random,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                65536,100,0,100,0,4,0,0
'Access specification name,default assignment
                64K 100% Read - Sequential,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                65536,100,100,0,0,4,0,0
'Access specification name,default assignment
                64K 0% Read - Sequential,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                65536,100,0,0,0,4,0,0
'Access specification name,default assignment
                128K 67% Read - Random,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                131072,100,67,100,0,4,0,0
'Access specification name,default assignment
                128K 100% Read - Random,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                131072,100,100,100,0,4,0,0
'Access specification name,default assignment
                128K 0% Read - Random,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                131072,100,0,100,0,4,0,0
'Access specification name,default assignment
                128K 100% Read - Sequential,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                131072,100,100,0,0,4,0,0
'Access specification name,default assignment
                128K 0% Read - Sequential,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                131072,100,0,0,0,4,0,0
'Access specification name,default assignment
                256K 67% Read - Random,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
```

```
                262144,100,67,100,0,4,0,0
'Access specification name,default assignment
                256K 100% Read - Random,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                262144,100,100,100,0,4,0,0
'Access specification name,default assignment
                256K 0% Read - Random,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                262144,100,0,100,0,4,0,0
'Access specification name,default assignment
                256K 100% Read - Sequential,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                262144,100,100,0,0,4,0,0
'Access specification name,default assignment
                256K 0% Read - Sequential,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                262144,100,0,0,0,4,0,0
'Access specification name,default assignment
                512K 67% Read - Random,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                524288,100,67,100,0,4,0,0
'Access specification name,default assignment
                512K 100% Read - Random,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                524288,100,100,100,0,4,0,0
'Access specification name,default assignment
                512K 0% Read - Random,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                524288,100,0,100,0,4,0,0
'Access specification name,default assignment
                512K 100% Read - Sequential,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                524288,100,100,0,0,4,0,0
'Access specification name,default assignment
                512K 0% Read - Sequential,NONE
'size,% of size,% reads,% random,delay,burst,align,reply
                524288,100,0,0,0,4,0,0
'END access specifications
Version 2006.07.27
```

DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INFORMATION AND TECHNOLOGY

ENTERPRISE INFRASTRUCTURE ENGINEERING

VA Enterprise IT Infrastructure Standard

Storage/SAN/Backup

Production v1.0

November 18, 2009

TABLE OF CONTENTS

1 Introduction 1

1.1 Purpose 1

1.2 Objectives 1

1.3 Scope 1

2 Standards 2

2.1 [Tier 1 storage service] 2

2.2 [Tier 2 storage service] 10

2.3 [Tier 3 storage service] 17

2.4 [General Storage Area Network (SAN)] 24

2.5 [General Backup and Archive standard] 29

3 Supporting Details for Standards 36

3.1 [Tier 1 storage service] 36

3.1.1 [Storage Subsystem Hardware (HW)] 36

3.1.2 [Mainframe support] 46

3.1.3 [Storage Management Software] 47

3.1.4 [Hardware/Software technical support] 50

3.1.5 [Hardware/software Installation] 53

3.1.6 [Training] 55

3.2 [Tier 2 storage service] 57

3.2.1 [Storage Subsystem Hardware (HW)] 57

3.2.2 [Storage Management Software] 67

3.2.3 [Hardware/Software technical support] 70

3.2.4 [Hardware/software Installation] 73

3.2.5 [Training] 75

3.3 [Tier 3 storage service] 77
3.3.1 [Storage Subsystem Hardware (HW)] 77
3.3.2 [Storage Management Software] 86
3.3.3 [Hardware/Software technical support] 89
3.3.4 [Hardware/software Installation] 92
3.3.5 [Training] 94
3.4 [General Storage Area Network (SAN)] 96
3.4.1 [LAN Connectivity] 96
3.4.2 [Fabric switch hardware (HW)] 97
3.4.3 [SAN Management Software] 101
3.4.4 [Hardware/Software technical support] 104
3.4.5 [Hardware/software Installation] 107
3.4.6 [Training] 110
3.5 [General Backup and Archive standard] 112
3.5.1 [Backup Method] 112
3.5.2 [Virtual tape library (VTL) hardware] 115
3.5.3 [Archive Hardware] 118
3.5.4 [Tape Library hardware] 121
3.5.5 [Backup Software/VTL/Archive/Tape library tool] 125
3.5.6 [Hardware/Software technical support] 128
3.5.7 [Hardware/software Installation] 131
3.5.8 [Training] 133
4 Taxonomy of Standards 135
Appendix A – Definitions 146
Appendix B – References 146
Appendix C – Acronyms 146
Appendix D – Contributors 146

1 INTRODUCTION

1.1 PURPOSE

A standard is a set of rules or requirements that are determined by a consensus opinion of subject matter experts and prescribe criteria for a product, process, test or procedure. The general benefits of a standard are quality, interchangeability of parts or systems, and consistency. Information Technology (IT) standards are based on business needs provided through or supported by IT Services. IT Services are designed to support business processes and are constructed from software, hardware and infrastructure components. Establishing and enforcing standards for the selection and configuration of these supporting components improves the maintainability, reliability and availability of IT Services within projected economic constraints in alignment with business needs.

This standards document lists the acceptable and recommended specifications for general and mission critical backend storage devices, storage area network, and backup solution. Sections include standard specifications for subject components, decisions supporting the standard specifications, guidelines or recommendations for implementing the standard specifications, and supplemental factors to consider when evaluating subject components. Other supplementary documents will provide guidance on procuring components that meet the standard specifications, guidance on integrating them with existing components, and explanation of how the subject components fit into the VA Architecture.

1.2 OBJECTIVES

This standard provides acceptable and recommended specifications to support:

- Solution Evaluation
- Requirement Evaluation
- Solution Design
- Solution Procurement and Bid Evaluation
- Evaluation of Architectural Specifications
- Provide vendor neutral or vendor specific where justified, for general and mission critical application backend storage devices, storage area network, and backup solution.

1.3 SCOPE

This standard applies to:

- These specifications are for new equipment targeting small facilities to regional data centers.
- Specifications will include all attributes necessary to specify general and mission critical application backend storage device, storage area network, and backup standard.

2 STANDARDS

2.1 [TIER 1 STORAGE SERVICE]

Tier 1 Services – Storage device supporting High and Extreme high Performance workloads.

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
1	Storage Subsystem Hardware (HW)	Workload	Capable to support Extreme High and High Workload such as OLTP databases (Cache/IDMS/Oracle/SQL) with 25,000 or more concurrent users
		Minimum IO/sec	100,000 SPC-1 IOPS™ as measured by SPC-1 benchmark (http://www.storageperformance.org/results/)
		Minimum Throughput	5,000 SPC-2 MBPS™ as measured by SPC-2 benchmark (http://www.storageperformance.org/results/)
		Storage unit uptime	5'9s uptime.
		Universal Device ID value (UDID)	Changeable LUN UDID value is required.
		Redundancy	Fully redundant power supplies, cooling fans, component controllers, and others. All controllers within a single module will automatically fail over and load balance with one another. Controller module will support a minimum of two controllers.
		FC - Hosts to Storage Connectivity	Storage subsystems must support minimum four 4-Gbit/s Fiber Channel ports. Ability to support ports expansion to meet Tier 1 performance requirements in the same unit(s).
			Minimum two redundant multi-path connections from Host to Storage device. The Host connectivity throughput and performance will not be degraded even if 50% of the Host connectivity is lost.
		iSCSI - Hosts to Storage Connectivity	Storage subsystems must support minimum 1 Gb Ethernet connectivity with link aggregation. 10 Gb Ethernet support is preferred. Controller module will

ID	Primary Attribute	Secondary Attribute	Specification
			support a minimum of four Ethernet ports. Ability to support ports expansion in the same unit(s). Support Jumbo frame and LACP protocol.
			Minimum two redundant multi-path connections from Host to Storage device. The Host connectivity throughput and performance will not be degraded even if 50% of the Host connectivity is lost.
		FICON connectivity	Storage subsystems must support FICON connectivity
		SCSI Initiator (Host Connections)	Support a minimum of 256
		Replication	Capable of synchronous and asynchronous replication with write order fidelity.
		LUN creation	Ability to create LUN across all spindles.
		LUN Expansion	Dynamic LUN expansion is required.
		Storage provisioning	Capable of over-provisioning or Over-allocation storage capacity that allows hosts to view more storage capacity than has been physically reserved on the storage array itself
		Tiering capability	Using policies to move inactive data to lower tier of storage
		Resource partitioning capability	Capable of isolating subsystem resources (such as Cache, Ports, CPU and Disk) and dedicate to particular host.
		Dynamically tuning	Dynamically tune and optimize storage subsystem components such as cache memory, disk, I/O ports in a single storage system is required.
		Backend Storage virtualization	Capable to connect other backend storage devices.
		Snapshots	Capable of creating point in time delta snapshot Capable of creating space efficient snapshots on an as needed basis versus snapshot space reservation
		Clones	Capable of creating point in time delta clone

ID	Primary Attribute	Secondary Attribute	Specification
			Capable of creating space efficient clones on an as needed basis versus snapshot space reservation. Immediate access to clones before it is completed.
		Storage device scale up capability	Ability to upgrade controller/controller module on storage device without forklift upgrade.
			Adding or upgrading storage subsystem components adhering to the required storage device uptime requirement and no data migration
		Supported Disk type	Ability to support sufficient disk drive technologies to meet Tier 1 performance requirements.
		Return disk option	Non-return disk option is required
		Interoperability - Industry standards	Each storage subsystem must provide Storage Management Initiative Specification (SMI-S) 1.1 conforming provider (http://www.snia.org/ctp/conformingproviders)
		Firmware and microcode upgrade or updates	Completely non-disruptive to operations firmware and microcode upgrade or updates for all components with zero downtime are required.
		Boot from SAN	Storage subsystem will support boot from San.
		Operating system and file system compatibility	Must support operating systems and their associated file systems as listed in the TRM.
		Applications compatibility (minimum)	Applications listed by VA Technical Reference Model (TRM) for enterprise deployment.
		Redundant Array of Independent Disk (RAID) levels	Minimum support for RAID 0+1/10/5/6 in same subsystems.
		RAID group size	Vendor offering must be able to meet storage capacity without exceeding 7 TB RAID group size and without exceeding 7 data drives.
		Power switches	Master power switches must be covered to prevent inadvertent activation.
		Standardized layouts	Components must be mounted in standardized configurations for all VA installations.

ID	Primary Attribute	Secondary Attribute	Specification
		Additional servers	Refer to Server Standard, Section Class C Server
		Role-based access	Solution must include security configurations that support role-based access required to limit functions during normal and COOP operation.
		Documentation	Provide detail design solution documents and drawings. All design methods and calculations to achieve the performance requirements must be clearly stated in the document. All assumptions if any must be included in the design document.
2	Mainframe support	Parallel Access Volume (PAV)	Ability to support/exploit Parallel Access Volume (PAV).
		FICON support	Minimum 8-Gbit/s FICON Channel ports. Ability to support additional ports in the same enclosure
		HiperPAV support	Ability to support HiperPAV. Dynamic capabilities associated with Parallel Access Volumes.
		SMF support	Support SMF – Must have compatibility with this activity log recording feature
		Emulation types	Must be able to emulate 3390 based count key data devices.
		Solid State devices (SSD) support on Mainframe	Must be able to support solid state devices on Mainframe. Tools are needed to analyze mainframe data for SSD exploitation.
		Dynamic Channel Reconfiguration support	Must be able to support Dynamic Channel Reconfiguration.
		MIDAW support	Must be able to support MIDAW facility
		Priority I/O Queuing	Must be able to support Priority I/O Queuing
3	Storage Management Software	Enterprise license not based on capacity	Software licenses provided must be perpetual with a five-year support and update subscription, with all licenses and rights transferred to the Government at the time the installation is completed. Licenses must be transferable without limitation and provisioned as a VA enterprise license, without additional storage allocation-based charges, such as per GB or TB.

ID	Primary Attribute	Secondary Attribute	Specification
		Interoperability	Management software must be listed as a Storage Networking Industry Association (SNIA) SMI-S 1.1 conforming client. (http://www.snia.org/forums/smi/tech_programs/ctp/smi_conform/smi_client/smi_client_definitions.
		Storage Reporting	Storage reporting components suitable for use in a fee for service, chargeback environment. Automated reports of storage allocations must be capable of being generated by non-IT staff. Must support ODBC and/or JDBC connectivity.
		Automated tools for LUN provisioning	The software should have automated tools to provision a large number of Disk Groups and LUNs. Similarly, an automated solution should be provided to configure hosts with large numbers of logical disks.
		Proactive monitoring and remote notification	The management tool must be capable of proactive monitoring and remote notification of system and application health. Must support ODBC and/or JDBC connectivity.
		Single storage management console	Storage hardware must be manageable from a single storage management application.
		Additional servers	Refer to Server Standard, Section Class C Server
		Management server security	Refer to Server Standard, Section Class C Server
		Data snapshot (local)	License and annual maintenance (5 years) as required for software to support array-based point-in-time data images suitable for use for administrative tasks such as online backup & testing with no impact to source data and minimal additional space requirements.
		Performance analysis	Performance management software to monitor, analyze and report on all solution components (i.e. from host to fabric to storage). This includes storage subsystems, software operations, SAN infrastructure, replication and telecommunications. Software should

ID	Primary Attribute	Secondary Attribute	Specification
			be able to identify and analyze response time, and other relevant metrics to enable identification and resolution of potential bottlenecks. The tool must support OpenVMS client operating system. All management software must be ODBC and/or JDBC connectivity.
		Storage Capacity planning	The software must be able to analyze current capacity and forecasts future system requirements. The software should be able to collect component data to project future usage of the storage system.
		Local copy	License and annual maintenance (5 years) as required for software to support local array-array LUN copy/replication.
		Consistent design	All software should use identical components where possible to facilitate common updates across the solution.
4	Hardware/Software technical support	Support procedures	Documented support/escalation procedure for all components of the solution.
		Support Availability	Software support required 24x7x365 for all software provided in the solution. License and annual maintenance 3 years with 2 extension years.
			Hardware Maintenance/Support 5 yr, 24x7x365. For issue impacting production operation, Tier2 or greater phone support response should be available within the first hour and less than 4 hours response for Engineer to bring parts onsite.
		License transfer	Licenses can be transferred without limitation within the Department of Veterans Affairs.
		OEM resources	Direct access to on-line OEM vendor support incident information and tracking.
		Support Interface	All VA datacenters must have access to incident information and tracking for all VA datacenters.
		Disruptive patches	Describe any type of updates/patch that would

ID	Primary Attribute	Secondary Attribute	Specification
			require a hosted service outage of the solution.
		SLAs	Documented Service Level Agreements (SLAs) for support requests.
		Professional services	Include cost of any professional services for services that must be completed by the vendor.
5	Hardware/software Installation	Installation	Provide hardware/software installation, including initial configuration, Storage Area Network configuration & knowledge transfer.
		Pre-configuration	Rack mount and configure the solution (including servers and storage where possible) prior to shipping it to the VA. This minimizes the on-site installation time as well as the number of crates and boxes that must be received and tracked by VA.
		Onsite impact	All on-site activities must be conducted in such a manner as to minimize the impact to normal information systems operations.
		Necessary software/hardware	Provide all necessary hardware and software, including all necessary cables and mounting hardware to make the Solution operational, except government-furnished property (GFP) referenced in GFP section.
		Delivery	Provide inside delivery, installation and insurance of all equipment to VA datacenters. The VA does not accept delivery of the equipment until acceptance testing is passed at all VA datacenters.
		Trash	Remove all trash associated with shipping, delivery and installation.
		OS installation and security	Refer to Server Standard, Section Class C Server
6	Training	Training Length	Provide equivalent of one hour of certified vendor classroom training for every TB of raw disk provided.
		Knowledge transfer	Allow VA staffs to shadow as activities occur to ensure

ID	Primary Attribute	Secondary Attribute	Specification
			that VA can assume operational responsibility for the delivered solution.
		Documentation	Provide electronic copies of all materials, manuals, worksheets, etc. used in the delivery of the solution.

2.2 [TIER 2 STORAGE SERVICE]

Tier 2 Services - Storage device supporting Medium Performance workloads.

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
1	Storage Subsystem Hardware (HW)	Workload	Capable to support Medium Performance such as Exchange Server, SQL Server, Virtual servers and generalized web servers with 25,000 or less concurrent users Workload.
		Minimum IO/sec	50,000 SPC-1 IOPS™ as measured by SPC-1 benchmark (http://www.storageperformance.org/results/)
		Minimum Throughput	1,000 SPC-2 MBPS™ as measured by SPC-2 benchmark (http://www.storageperformance.org/results/)
		Storage unit uptime	4'9s uptime.
		Universal Device ID value (UDID)	Changeable LUN UDID value is required.
		Redundancy	Fully redundant power supplies, cooling fans, component controllers, and others. All controllers within a single module will automatically fail over and load balance with one another. Controller module will support a minimum of two controllers.
		FC - Hosts to Storage Connectivity	Storage subsystems must support minimum four 4-Gbit/s Fiber Channel ports. Ability to support ports expansion to meet Tier 1 performance requirements in the same unit(s).
			Minimum two redundant multi-path connections from Host to Storage device. The Host connectivity throughput and performance will not be degraded even if 50% of the Host connectivity is lost.
		iSCSI - Hosts to Storage Connectivity	Storage subsystems must support minimum 1 Gb Ethernet connectivity with link aggregation. 10 Gb Ethernet support is preferred. Controller module will support a minimum of four Ethernet ports. Ability to support ports expansion in the same unit(s). Support Jumbo frame and LACP protocol.
			Minimum two redundant multi-path connections from Host to Storage device. The Host connectivity

ID	Primary Attribute	Secondary Attribute	Specification
			throughput and performance will not be degraded even if 50% of the Host connectivity is lost.
		SCSI Initiator (Host Connections)	Support a minimum of 256
		Replication	Capable of synchronous and asynchronous replication with write order fidelity.
		LUN creation	Ability to create LUN across all spindles.
		LUN Expansion	Dynamic LUN expansion is required.
		Storage provisioning	Capable of over-provisioning or Over-allocation storage capacity that allows hosts to view more storage capacity than has been physically reserved on the storage array itself
		Tiering capability	Using policies to move inactive data to lower tier of storage
		Deduplication	Minimum support post process deduplication.
		Snapshots	Capable of creating point in time delta snapshot Capable of creating space efficient snapshots on an as needed basis versus snapshot space reservation
		Clones	Capable of creating point in time delta clone Capable of creating space efficient clones on an as needed basis versus snapshot space reservation. Immediate access to clones before it is completed.
		Storage device scale up capability	Ability to upgrade controller/controller module on storage device without forklift upgrade.
			Adding or upgrading storage subsystem components adhering to the required storage device uptime requirement and no data migration
		Supported Disk type	Ability to support sufficient disk drive technologies to meet Tier 2 performance requirements.
		Return disk option	Non-return disk option is required
		Interoperability -	Each storage subsystem must provide Storage

ID	Primary Attribute	Secondary Attribute	Specification
		Industry standards	Management Initiative Specification (SMI-S) 1.1 conforming provider (http://www.snia.org/ctp/conformingproviders)
		Firmware and microcode upgrade or updates	Completely non-disruptive to operations firmware and microcode upgrade or updates for all components with zero downtime are required.
		Boot from SAN	Storage subsystem will support boot from San.
		Operating system and file system compatibility	Must support operating systems and their associated file systems as listed in the TRM.
		Applications compatibility (minimum)	Applications listed by VA Technical Reference Model (TRM) for enterprise deployment.
		Redundant Array of Independent Disk (RAID) levels	Minimum support for RAID 0+1/10/5/6 in same subsystems.
		RAID group size	Vendor offering must be able to meet storage capacity without exceeding 7 TB RAID group size and without exceeding 7 data drives.
		Power switches	Master power switches must be covered to prevent inadvertent activation.
		Standardized layouts	Components must be mounted in standardized configurations for all VA installations.
		Additional servers	Refer to Server Standard, Section Class C Server
		Role-based access	Solution must include security configurations that support role-based access required to limit functions during normal and COOP operation.
		Documentation	Provide detail design solution documents and drawings. All design methods and calculations to achieve the performance requirements must be clearly stated in the document. All assumptions if any must be included in the design document
2	Storage Management Software	Enterprise license not based on capacity	Software licenses provided must be perpetual with a five-year support and update subscription, with all licenses and rights transferred to the Government at

ID	Primary Attribute	Secondary Attribute	Specification
			the time the installation is completed. Licenses must be transferable without limitation and provisioned as a VA enterprise license, without additional storage allocation-based charges, such as per GB or TB.
		Interoperability	Management software must be listed as a Storage Networking Industry Association (SNIA) SMI-S 1.1 conforming client. (http://www.snia.org/forums/smi/tech_programs/ctp/smi_conform/smi_client/smi_client_definitions.
		Storage Reporting	Storage reporting components suitable for use in a fee for service, chargeback environment. Automated reports of storage allocations must be capable of being generated by non-IT staff. Must support ODBC and/or JDBC connectivity.
		Automated tools for LUN provisioning	The software should have automated tools to provision a large number of Disk Groups and LUNs. Similarly, an automated solution should be provided to configure hosts with large numbers of logical disks.
		Proactive monitoring and remote notification	The management tool must be capable of proactive monitoring and remote notification of system and application health. Must support ODBC and/or JDBC connectivity.
		Single storage management console	Storage hardware must be manageable from a single storage management application.
		Additional servers	Refer to Server Standard, Section Class C Server
		Management server security	Refer to Server Standard, Section Class C Server
		Data snapshot (local)	License and annual maintenance (5 years) as required for software to support array-based point-in-time data images suitable for use for administrative tasks such as online backup & testing with no impact to source data and minimal additional space requirements.
		Performance analysis	Performance management software to monitor,

ID	Primary Attribute	Secondary Attribute	Specification
			analyze and report on all solution components (i.e. from host to fabric to storage). This includes storage subsystems, software operations, SAN infrastructure, replication and telecommunications. Software should be able to identify and analyze response time, and other relevant metrics to enable identification and resolution of potential bottlenecks. The tool must support OpenVMS client operating system. All management software must be ODBC and/or JDBC connectivity.
		Storage Capacity planning	The software must be able to analyze current capacity and forecasts future system requirements. The software should be able to collect component data to project future usage of the storage system.
		Local copy	License and annual maintenance (5 years) as required for software to support local array-array LUN copy/replication.
		Consistent design	All software should use identical components where possible to facilitate common updates across the solution.
3	Hardware/Software technical support	Support procedures	Documented support/escalation procedure for all components of the solution.
		Support Availability	Software support required 24x7x365 for all software provided in the solution. License and annual maintenance 3 years with 2 extension years.
			Hardware Maintenance/Support 5 yr, 24x7x365, 4 hour response time is required.
		License transfer	Licenses can be transferred without limitation within the Department of Veterans Affairs.
		OEM resources	Direct access to on-line OEM vendor support incident information and tracking.
		Support Interface	All VA datacenters must have access to incident information and tracking for all VA datacenters.
		Disruptive patches	Describe any type of updates/patch that would

ID	Primary Attribute	Secondary Attribute	Specification
			require a hosted service outage of the solution.
		SLAs	Documented Service Level Agreements (SLAs) for support requests.
		Professional services	Include cost of any professional services for services that must be completed by the vendor.
4	Hardware/software Installation	Installation	Provide hardware/software installation, including initial configuration, Storage Area Network configuration & knowledge transfer.
		Pre-configuration	Rack mount and configure the solution (including servers and storage where possible) prior to shipping it to the VA. This minimizes the on-site installation time as well as the number of crates and boxes that must be received and tracked by VA.
		Onsite impact	All on-site activities must be conducted in such a manner as to minimize the impact to normal information systems operations.
		Necessary software/hardware	Provide all necessary hardware and software, including all necessary cables and mounting hardware to make the Solution operational, except government-furnished property (GFP) referenced in GFP section.
		Delivery	Provide inside delivery, installation and insurance of all equipment to VA datacenters. The VA does not accept delivery of the equipment until acceptance testing is passed at all VA datacenters.
		Trash	Remove all trash associated with shipping, delivery and installation.
		OS installation and security	Refer to Server Standard, Section Class C Server
5	Training	Training Length	Provide equivalent of one hour of certified vendor classroom training for every TB of raw disk provided.
		Knowledge transfer	Allow VA staffs to shadow as activities occur to ensure

ID	Primary Attribute	Secondary Attribute	Specification
			that VA can assume operational responsibility for the delivered solution.
		Documentation	Provide electronic copies of all materials, manuals, worksheets, etc. used in the delivery of the solution.

2.3 [TIER 3 STORAGE SERVICE]

Tier 3 Services - Storage device supporting Low and small Performance workloads.

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
1	Storage Subsystem Hardware (HW)	Workload	Capable to support Small and Low Performance Workload. Target performance would be retrieval of data file of 10 MB within 60 seconds of request.
		Minimum IO/sec	20,000 SPC-1 IOPS™ as measured by SPC-1 benchmark (http://www.storageperformance.org/results/))
		Minimum Throughput	1,000 or less SPC-2 MBPS™ as measured by SPC-2 benchmark (http://www.storageperformance.org/results/)
		Storage unit uptime	4'9s uptime.
		Universal Device ID value (UDID)	Not applicable.
		Redundancy	Fully redundant power supplies, cooling fans, component controllers, and others. All controllers within a single module will automatically fail over and load balance with one another. Controller module will support a minimum of two controllers.
		FC - Hosts to Storage Connectivity	Storage subsystems must support minimum four 4-Gbit/s Fiber Channel ports. Ability to support ports expansion to meet Tier 1 performance requirements in the same unit(s).
			Minimum two redundant multi-path connections from Host to Storage device. The Host connectivity throughput and performance will not be degraded even if 50% of the Host connectivity is lost.
		iSCSI - Hosts to Storage Connectivity	Storage subsystems must support minimum 1 Gb Ethernet connectivity with link aggregation. 10 Gb Ethernet support is preferred. Controller module will support a minimum of four Ethernet ports. Ability to support ports expansion in the same unit(s). Support Jumbo frame and LACP protocol.
			Minimum two redundant multi-path connections from Host to Storage device. The Host connectivity

ID	Primary Attribute	Secondary Attribute	Specification
			throughput and performance will not be degraded even if 50% of the Host connectivity is lost.
		SCSI Initiator (Host Connections)	Support a minimum of 256
		Replication	Capable of synchronous and asynchronous replication with write order fidelity.
		LUN creation	Ability to create LUN across all spindles.
		LUN Expansion	Dynamic LUN expansion is required.
		Storage provisioning	Capable of over-provisioning or Over-allocation storage capacity that allows hosts to view more storage capacity than has been physically reserved on the storage array itself
		Tiering capability	Using policies to move inactive data to lower tier of storage
		Deduplication	Minimum support post process deduplication.
		Snapshots	Capable of creating point in time delta snapshot Capable of creating space efficient snapshots on an as needed basis versus snapshot space reservation
		Clones	Capable of creating point in time delta clone Capable of creating space efficient clones on an as needed basis versus snapshot space reservation. Immediate access to clones before it is completed.
		Storage device scale up capability	Not applicable.
		Supported Disk type	Ability to support sufficient disk drive technologies to meet Tier 3 performance requirements.
		Return disk option	Non-return disk option is required
		Interoperability - Industry standards	Each storage subsystem must provide Storage Management Initiative Specification (SMI-S) 1.1 conforming provider (http://www.snia.org/ctp/conformingproviders)

ID	Primary Attribute	Secondary Attribute	Specification
		Firmware and microcode upgrade or updates	Completely non-disruptive to operations firmware and microcode upgrade or updates for all components with zero downtime are required.
		Boot from SAN	Storage subsystem will support boot from San.
		Operating system and file system compatibility	Must support operating systems and their associated file systems as listed in the TRM.
		Applications compatibility (minimum)	Applications listed by VA Technical Reference Model (TRM) for enterprise deployment.
		Redundant Array of Independent Disk (RAID) levels	Minimum support for RAID 0+1/10/5/6 in same subsystems.
		RAID group size	Vendor offering must be able to meet storage capacity without exceeding 7 TB RAID group size and without exceeding 7 data drives.
		Power switches	Master power switches must be covered to prevent inadvertent activation.
		Standardized layouts	Components must be mounted in standardized configurations for all VA installations.
		Additional servers	Refer to Server Standard, Section Class C Server
		Role-based access	Solution must include security configurations that support role-based access required to limit functions during normal and COOP operation.
		Documentation	Provide detail design solution documents and drawings. All design methods and calculations to achieve the performance requirements must be clearly stated in the document. All assumptions if any must be included in the design document
2	Storage Management Software	Enterprise license not based on capacity	Software licenses provided must be perpetual with a five-year support and update subscription, with all licenses and rights transferred to the Government at the time the installation is completed. Licenses must be transferable without limitation and provisioned as a VA enterprise license, without additional storage

ID	Primary Attribute	Secondary Attribute	Specification
			allocation-based charges, such as per GB or TB.
		Interoperability	Management software must be listed as a Storage Networking Industry Association (SNIA) SMI-S 1.1 conforming client. (http://www.snia.org/forums/smi/tech_programs/ctp/smi_conform/smi_client/smi_client_definitions.
		Storage Reporting	Storage reporting components suitable for use in a fee for service, chargeback environment. Automated reports of storage allocations must be capable of being generated by non-IT staff. Must support ODBC and/or JDBC connectivity.
		Automated tools for LUN provisioning	The software should have automated tools to provision a large number of Disk Groups and LUNs. Similarly, an automated solution should be provided to configure hosts with large numbers of logical disks.
		Proactive monitoring and remote notification	The management tool must be capable of proactive monitoring and remote notification of system and application health. Must support ODBC and/or JDBC connectivity.
		Single storage management console	Storage hardware must be manageable from a single storage management application.
		Additional servers	Refer to Server Standard, Section Class C Server
		Management server security	Refer to Server Standard, Section Class C Server
		Data snapshot (local)	License and annual maintenance (5 years) as required for software to support array-based point-in-time data images suitable for use for administrative tasks such as online backup & testing with no impact to source data and minimal additional space requirements.
		Performance analysis	Performance management software to monitor, analyze and report on all solution components (i.e. from host to fabric to storage). This includes storage subsystems, software operations, SAN infrastructure,

ID	Primary Attribute	Secondary Attribute	Specification
			replication and telecommunications. Software should be able to identify and analyze response time, and other relevant metrics to enable identification and resolution of potential bottlenecks. The tool must support OpenVMS client operating system. All management software must be ODBC and/or JDBC connectivity.
		Storage Capacity planning	The software must be able to analyze current capacity and forecasts future system requirements. The software should be able to collect component data to project future usage of the storage system.
		Local copy	License and annual maintenance (5 years) as required for software to support local array-array LUN copy/replication.
		Consistent design	All software should use identical components where possible to facilitate common updates across the solution.
3	Hardware/Software technical support	Support procedures	Documented support/escalation procedure for all components of the solution.
		Support Availability	Software support required 24x7x365 for all software provided in the solution. License and annual maintenance 3 years with 2 extension years.
			Hardware Maintenance/Support 5 yr, 24x7x365, 4 hour response time is required.
		License transfer	Licenses can be transferred without limitation within the Department of Veterans Affairs.
		OEM resources	Direct access to on-line OEM vendor support incident information and tracking.
		Support Interface	All VA datacenters must have access to incident information and tracking for all VA datacenters.
		Disruptive patches	Describe any type of updates/patch that would require a hosted service outage of the solution.
		SLAs	Documented Service Level Agreements (SLAs) for

ID	Primary Attribute	Secondary Attribute	Specification
			support requests.
		Professional services	Include cost of any professional services for services that must be completed by the vendor.
4	Hardware/software Installation	Installation	Provide hardware/software installation, including initial configuration, Storage Area Network configuration & knowledge transfer.
		Pre-configuration	Rack mount and configure the solution (including servers and storage where possible) prior to shipping it to the VA. This minimizes the on-site installation time as well as the number of crates and boxes that must be received and tracked by VA.
		Onsite impact	All on-site activities must be conducted in such a manner as to minimize the impact to normal information systems operations.
		Necessary software/hardware	Provide all necessary hardware and software, including all necessary cables and mounting hardware to make the Solution operational, except government-furnished property (GFP) referenced in GFP section.
		Delivery	Provide inside delivery, installation and insurance of all equipment to VA datacenters. The VA does not accept delivery of the equipment until acceptance testing is passed at all VA datacenters.
		Trash	Remove all trash associated with shipping, delivery and installation.
		OS installation and security	Refer to Server Standard, Section Class C Server
5	Training	Training Length	Provide equivalent of one hour of certified vendor classroom training for every TB of raw disk provided.
		Knowledge transfer	Allow VA staffs to shadow as activities occur to ensure that VA can assume operational responsibility for the delivered solution.

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
		Documentation	Provide electronic copies of all materials, manuals, worksheets, etc. used in the delivery of the solution.

2.4 [GENERAL STORAGE AREA NETWORK (SAN)]

Attributes necessary to specify general storage area network fabric for Data Center

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
1	LAN Connectivity	IP Connectivity between Hosts and Storage device	Minimum 1 Gb Ethernet and 10 Gb Ethernet is preferred. Support Jumbo frame and LACP protocol.
			Support multi-pathing from Hosts and Storage devices.
			Storage Data connection should be logically separate from production LAN data connection.
			Primary storage data connection should be logically separate from replication data connection.
2	Fabric switch hardware (HW)	Fabric Connectivity between Hosts and Storage device	Redundant Switch Control (Supervisor) Card
			Fiber Channel Protocol
			Minimum 4-Gbit/s Fiber Channel Ports
			All fiber Channel switch ports will be autosensing to 1, 2, 4 or 8Gb
		Interoperability	Compatible with equipment from Cisco, Brocade and Nortel hardware.
		Fabric Isolation	Local SAN fabric must be isolated from replication SAN fabric
		Capacity “Throughput”	Isolate data and devices within a fabric, and configurable throughput for specific applications. Supports at least 1 TBps of internal bandwidth in a single chassis (switch enclosure).
		Capacity “Ports”	384 FC ports in a single chassis (switch enclosure). Able to provision additional SAN ports without interruption.
		Port virtualization	Support N Port Virtualization.
		Manageability	Manageable from a single application.
		Fully redundant	Provide fully redundant configuration

ID	Primary Attribute	Secondary Attribute	Specification
		configuration	
		Oversubscription	Provide no more than 4:1 over subscription at 4 Gbps.
		Fabric	SAN switch shall support redundant fabrics.
		Automated monitoring	SAN switches must implement automated monitoring and phone-home support configurations over IP.
		Current generation equipment	Fiber channel switches and/or components must not be listed on vendor websites as “end of life” or “end of sale” or “end of service life”. The initial hardware general availability date should be less than 5 years from the proposal submission date.
		Additional ports	Solution must provision additional SAN ports required to fully connect solution components (storage subsystems, inter-switch links, management hosts, replication hardware, etc) in addition to host requirements.
		Rack Configuration	Provide appropriate 4 posts (42 or 47 U) with sidewalls.
		Manageable power supplies	Redundant IP Manageable & Accessible Power Distribution Unit (PDUs) sufficient to power all units in the rack.
		Cooling	Fans (N+1) on switch and cabinet to support airflow requirements.
		Physical layout	All components must be easily accessible without having to de-install, disconnect or remove other components so that service can be easily accomplished.
		Standardized layouts	Components must be mounted in standardized configurations for all VA installations.
		Additional servers	Refer to Server Standard, Section Class C Server
		Role-based access	Solution must include security configurations that support role-based access required to limit functions

ID	Primary Attribute	Secondary Attribute	Specification
			during normal and COOP operation.
3	SAN Management Software	Management Software	Enterprise level SAN management software Automatic configuration checking for SAN configuration, updates and reconfigurations. Automatic discover of equipment connected to the SAN Manage multiple devices in a selected domain. Wizards for common tasks such as zone configuration, , Fiber Channel over IP (FCIP) tunnels, and access control lists (ACLs) Fabric Interoperability – work with SAN switches regardless of vendor Must support ODBD and JDBC connectivity
		SAN Reporting	SAN reporting components suitable for use in an enterprise environment. Automated reports of storage allocations must be capable of being generated by non-IT staff. Must support ODBC and/or JDBC connectivity.
		Proactive monitoring and remote notification	The management tool must be capable of proactive monitoring and remote notification of system and application health. Must support ODBC and/or JDBC connectivity.
		Performance monitoring	Performance statistics for Inter-Switch Links (ISLs), host and storage device connections, and traffic between specific Fiber Channel sources and destinations (flows) Ability to set performance threshold based on manual entry or calculated based on previous measurements. Historical performance reports and graphs over daily, weekly, monthly, and yearly intervals; Top 10 and daily summary reports for all ISLs, hosts, storage connections, and flows. Performance reports should be accessible without

ID	Primary Attribute	Secondary Attribute	Specification
			privileged access to the SAN switch.
		Single SAN management console	SAN hardware must be manageable from a single storage management application.
		Additional servers	Refer to Server Standard, Section Class C Server
		Management server security	Refer to Server Standard, Section Class C Server
		Consistent design	All software should use identical components where possible to facilitate common updates across the solution.
4	Hardware/Software technical support	Support procedures	Documented support/escalation procedure for all components of the solution.
		Support Availability	Software support required 24x7x365 for all software provided in the solution. License and annual maintenance 3 years with 2 extension years.
			Hardware Maintenance/Support 5 yr, 24x7x365, 4 hour response time is required.
		License transfer	Licenses can be transferred without limitation within the Department of Veterans Affairs.
		OEM resources	Direct access to on-line OEM vendor support incident information and tracking.
		Support Interface	All VA datacenters must have access to incident information and tracking for all VA datacenters.
		Disruptive patches	Describe any type of updates/patch that would require a hosted service outage of the solution.
		SLAs	Documented Service Level Agreements (SLAs) for support requests.
		Professional services	Include cost of any professional services for services that must be completed by the vendor.
5	Hardware/software	Installation	Provide hardware/software installation, including

ID	Primary Attribute	Secondary Attribute	Specification
	Installation		initial configuration, Storage Area Network configuration & knowledge transfer.
		Pre-configuration	Rack mount and configure the solution (including servers and storage where possible) prior to shipping it to the VA. This minimizes the on-site installation time as well as the number of crates and boxes that must be received and tracked by VA.
		Onsite impact	All on-site activities must be conducted in such a manner as to minimize the impact to normal information systems operations.
		Necessary software/hardware	Provide all necessary hardware and software, including all necessary cables and mounting hardware to make the Solution operational, except government-furnished property (GFP) referenced in GFP section.
		Delivery	Provide inside delivery, installation and insurance of all equipment to VA datacenters. The VA does not accept delivery of the equipment until acceptance testing is passed at all VA datacenters.
		Trash	Remove all trash associated with shipping, delivery and installation.
		OS installation and security	Refer to Server Standard, Section Class C Server
		Single-initiator zoning	Hosts shall be connected using single-initiator zoning configuration.
6	Training	Training Length	Provide equivalent of one day of certified vendor classroom training for every 24 fiber channel ports provided.
		Knowledge transfer	Work with VA staff as activities occur to ensure that VA can assume operational responsibility for the delivered solution.
		Documentation	Provide electronic copies of all materials, manuals, worksheets, etc. used in the delivery of the solution.

2.5 [GENERAL BACKUP AND ARCHIVE STANDARD]

Attributes necessary to specify general backup and Archive solution for Data Center

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
1	Backup Method	Tape	Direct tape backup from Primary storage
			Snapshot from Primary disk to secondary disk and backup to tape. Offload backup resources from primary storage device to secondary storage device (VTL or disk) is preferred
		Disk (Tapeless)	Backup from Primary disk to secondary disk such as Virtual tape library (VTL) with deduplication solution that meets all other backup requirements including retention and offsite storage policy
			Continuous Data Protection (CDP) is preferred for stringent SLA, RPO, and RTO requirements and the ability to recover ANY point in time
			Support Asynchronous replication with deduplicated data is preferred.
		Archive	Long term Data Archiving solution must meet OGC VA Litigation requirements
			Do not access data frequently
2	Virtual tape library (VTL) hardware	Technology	Support Massive Array of Idle Disks (MAID)
		Disk health monitoring	Capable of pro-actively disks monitoring and detecting potential drive failures before it occurs.
		Deduplication	Minimum support post process deduplication.
		Replication	Support Asynchronous replication with deduplicated data
		Raw Storage Capacity	Up to 896 TB per cabinet
		Number of Emulated Tape Libraries	1 to 8

ID	Primary Attribute	Secondary Attribute	Specification
		Number of Emulated Tape Drives	1 to 28 standard (1-512 with HPCM option)
		Number of Virtual Tape Cartridges	Up to 8192
		Connectivity	Minimum four FC connectivity of 4 GigE ports per system
		Redundancy	Redundant fan, N+1 Redundancy, Hot-Swappable Power Supplies
3	Archive Hardware	Technology	Support Massive Array of Idle Disks (MAID)
		Disk health monitoring	Capable of pro-actively disks monitoring and detecting potential drive failures before it occurs.
		Data Storage Architecture	Support write-once-read-many (WORM) and Write Once Read Occasionally (WORO)
		Deduplication	Minimum support post process deduplication.
		Replication	Support Asynchronous replication with deduplicated data
		Protocol Support	CIFS,NFS V2 + V3, TCP/IP
		Number of Files	Up to 1.5 Billion files
		File Size	Up to 1.2TB file size
		Raw Storage Capacity	Up to 896 TB per cabinet
		Number of drives	Single Cabinet Up to 896 drives
		Connectivity	Minimum four FC connectivity of 4 GigE ports per system
		Redundancy	Redundant fan, N+1 Redundancy, Hot-Swappable Power Supplies
4	Tape Library hardware	Interoperability -	Tape Library must provide for tape drives with

ID	Primary Attribute	Secondary Attribute	Specification
		Industry standards	minimum 800 GB uncompressed and throughput minimum of 120 MB/sec. Tape Library drives must be capable of encryption with minimum 1TB tape capacity and throughput minimum of 120 MB/sec. (FIPS 140-2, Level 3)
		Compatibility	Tape library must be capable of reading previously written tapes in the following formats: DLT and LTO.
		Backup SAN	Solution must provision SAN/network components as required to meet performance requirements and isolate backup traffic from normal production traffic.
		Connectivity	Fiber Channel, FICON, ESCON
		Fully redundant configuration	Provide fully redundant configuration such as ports, robots, tape drives, power supplies.
		Current generation equipment	Tape libraries and/or components must not be listed on vendor websites as “end of life” or “end of sale”. The initial hardware general availability date should be less than 5 years from the proposal submission date.
		Library Capacity (throughput)	Minimum throughput of 16 TB per hour
		Capacity (slots)	Solution must provide a minimum of 500 active tape slots
		Scalability (throughput)	Minimum scalability of 20 TB per hour
		Scalability (slots)	Solution must provide the ability to expand to 100% of minimum number of tape slots.
		Rack Configuration	Provide appropriate 4 posts (42 or 47 U) with sidewalls.
		Manageable power supplies	Redundant IP Manageable & Accessible Power Distribution Unit (PDUs) sufficient to power all units in the rack.

ID	Primary Attribute	Secondary Attribute	Specification
		Cooling	N + 1 Fans to support airflow requirements.
		Physical layout	All components must be easily accessible without having to de-install, disconnect or remove other components so that service can be easily accomplished.
		Size	Equipment footprint of less than 60 square feet in fully-scaled configuration.
		Standardized layouts	Components must be mounted in standardized configurations for all VA installations.
		Additional servers	Refer to Server Standard, Section Class C Server.
		Online maintenance	Ability to make hardware changes, repairs and expansion without impacting daily operations.
5	Backup Software/VTL/Archive/ Tape library tool	Backup Software	Provide Enterprise level backup software with ODBC and JDBC connectivity.
			Support Open VMS client and Open VMS Scripting is required
			Software with source and target Deduplication capability. Support Global Deduplication is preferred.
			Capable of synthetic backup
			NDMP backup and restore capable of performing block level backup and file level restore
			Capable of creating snapshots and clones. Support Continuous Data Protection (CDP)
		Tape Library management tool	Provide Enterprise level Tape Library management software. Compatibility with tape backup software. Listed on the VA Technical Reference Model (TRM) is preferred
		Encryption	Enterprise Backup software encryption and Enterprise

ID	Primary Attribute	Secondary Attribute	Specification
			encryption key management system complying with FIPS 140-2 level 3 standards without regard to application, operating system or primary storage device.
		Compatibility	Compatibility with operating systems listed on the VA Technical Reference Model (TRM)
		Scripting	Compatibility with operating systems listed on the VA Technical Reference Model (TRM)
		Proactive monitoring and remote notification	The software and management tool must be capable of proactive monitoring and remote notification of system and application health. Must support ODBC and/or JDBC connectivity.
		Role-based access	Solution must include security configurations that support role-based access required to limit functions during normal and COOP operation.
		Manageability	Manageable from a single application provided as part of the solution.
		Additional servers	Refer to Server Standard, Section Class C Server.
		Management server security	Refer to Server Standard, Section Class C Server.
		Consistent design	All software should use identical components where possible to facilitate common updates across the solution.
6	Hardware/Software technical support	Support procedures	Documented support/escalation procedure for all components of the solution.
		Support Availability	Software support required 24x7x365 for all software provided in the solution. License and annual maintenance 3 years with 2 extension years.
			Hardware Maintenance/Support 5 yr, 24x7x365, 4 hour response time is required.
		License transfer	Licenses can be transferred without limitation within the Department of Veterans Affairs.

ID	Primary Attribute	Secondary Attribute	Specification
		OEM resources	Direct access to on-line OEM vendor support incident information and tracking.
		Support Interface	All VA datacenters must have access to incident information and tracking for all VA datacenters.
		Disruptive patches	Describe any type of updates/patch that would require a hosted service outage of the solution.
		SLAs	Documented Service Level Agreements (SLAs) for support requests.
		Professional services	Include cost of any professional services for services that must be completed by the vendor.
7	Hardware/software Installation	Installation	Provide hardware/software installation, including initial configuration, Storage Area Network configuration & knowledge transfer.
		Pre-configuration	Rack mount and configure the solution (including servers and storage where possible) prior to shipping it to the VA. This minimizes the on-site installation time as well as the number of crates and boxes that must be received and tracked by VA.
		Onsite impact	All on-site activities must be conducted in such a manner as to minimize the impact to normal information systems operations.
		Necessary software/hardware	Provide all necessary hardware and software, including all necessary cables and mounting hardware to make the Solution operational, except government-furnished property (GFP) referenced in GFP section.
		Delivery	Provide inside delivery, installation and insurance of all equipment to VA datacenters. The VA does not accept delivery of the equipment until acceptance testing is passed at all VA datacenters.
		Trash	Remove all trash associated with shipping, delivery and installation.

ID	Primary Attribute	Secondary Attribute	Specification
		OS installation and security	Refer to Server Standard, Section Class C Server.
8	Training	Training Length	Provide equivalent of one day of certified vendor classroom training for every installed tape drive or every 12TB of VTL and Archive storage space.
		Knowledge transfer	Work with VA staff as activities occur to ensure that VA can assume operational responsibility for the delivered solution.
		Documentation	Provide electronic copies of all materials, manuals, worksheets, etc. used in the delivery of the solution.

3 SUPPORTING DETAILS FOR STANDARDS

3.1 [TIER 1 STORAGE SERVICE]

3.1.1 [STORAGE SUBSYSTEM HARDWARE (HW)]

STANDARD

ID	*Secondary Attribute*	*Specification*
	Workload	Capable to support Extreme High and High Workload such as OLTP databases (Cache/IDMS/Oracle/SQL) with 25,000 or more concurrent users
	Minimum IO/sec	100,000 SPC-1 IOPS™ as measured by SPC-1 benchmark (http://www.storageperformance.org/results/)
	Minimum Throughput	5,000 SPC-2 MBPS™ as measured by SPC-2 benchmark (http://www.storageperformance.org/results/)
	Storage unit uptime	5'9s uptime.
	Universal Device ID value (UDID)	Changeable LUN UDID value is required.
	Redundancy	Fully redundant power supplies, cooling fans, component controllers, and others. All controllers within a single module will automatically fail over and load balance with one another. Controller module will support a minimum of two controllers.
	FC - Hosts to Storage Connectivity	Storage subsystems must support minimum four 4-Gbit/s Fiber Channel ports. Ability to support ports expansion to meet Tier 1 performance requirements in the same unit(s).
		Minimum two redundant multi-path connections from Host to Storage device. The Host connectivity throughput and performance will not be degraded even if 50% of the Host connectivity is lost.
	iSCSI - Hosts to Storage Connectivity	Storage subsystems must support minimum 1 Gb Ethernet connectivity with link aggregation. 10 Gb Ethernet support is preferred. Controller module will support a minimum of four Ethernet ports. Ability to support ports expansion in the same unit(s). Support Jumbo frame and LACP protocol.
		Minimum two redundant multi-path connections from Host to Storage device. The Host connectivity throughput and performance will not be degraded even if 50% of the Host connectivity is lost.

	FICON connectivity	Storage subsystems must support FICON connectivity
	SCSI Initiator (Host Connections)	Support a minimum of 256
	Replication	Capable of synchronous and asynchronous replication with write order fidelity.
	LUN creation	Ability to create LUN across all spindles.
	LUN Expansion	Dynamic LUN expansion is required.
	Storage provisioning	Capable of over-provisioning or Over-allocation storage capacity that allows hosts to view more storage capacity than has been physically reserved on the storage array itself
	Tiering capability	Using policies to move inactive data to lower tier of storage
	Resource partitioning capability	Capable of isolating subsystem resources (such as Cache, Ports, CPU and Disk) and dedicate to particular host.
	Dynamically tuning	Dynamically tune and optimize storage subsystem components such as cache memory, disk, I/O ports in a single storage system is required.
	Backend Storage virtualization	Capable to connect other backend storage devices
	Snapshots	Capable of creating point in time delta snapshot Capable of creating space efficient snapshots on an as needed basis versus snapshot space reservation
	Clones	Capable of creating point in time delta clone Capable of creating space efficient clones on an as needed basis versus snapshot space reservation. Immediate access to clones before it is completed.
	Storage device scale up capability	Ability to upgrade controller/controller module on storage device without forklift upgrade.
		Adding or upgrading storage subsystem components adhering to the required storage device uptime requirement and no data migration
	Supported Disk type	Ability to support sufficient disk drive technologies to meet Tier 1 performance requirements.
	Return disk option	Non-return disk option is required

	Interoperability - Industry standards	Each storage subsystem must provide Storage Management Initiative Specification (SMI-S) 1.1 conforming provider (http://www.snia.org/ctp/conformingproviders)
	Firmware and microcode upgrade or updates	Completely non-disruptive to operations firmware and microcode upgrade or updates for all components with zero downtime are required.
	Boot from SAN	Storage subsystem will support boot from San.
	Operating system and file system compatibility	Must support operating systems and their associated file systems as listed in the TRM.
	Applications compatibility (minimum)	Applications listed by VA Technical Reference Model (TRM) for enterprise deployment.
	Redundant Array of Independent Disk (RAID) levels	Minimum support for RAID 0+1/10/5/6 in same subsystems.
	RAID group size	Vendor offering must be able to meet storage capacity without exceeding 7 TB RAID group size and without exceeding 7 data drives.
	Power switches	Master power switches must be covered to prevent inadvertent activation.
	Standardized layouts	Components must be mounted in standardized configurations for all VA installations.
	Additional servers	Refer to Server Standard, Section Class C Server
	Role-based access	Solution must include security configurations that support role-based access required to limit functions during normal and COOP operation.
	Documentation	Provide detail design solution documents and drawings. All design methods and calculations to achieve the performance requirements must be clearly stated in the document. All assumptions if any must be included in the design document

EXPLANATION OF STANDARD

Workload – The storage system must be able to handle the amount of data and transactions that accompany large shared enterprise level applications with high amounts of transactions and large amounts of I/O. Capable of supporting Extreme High and High performance workloads such as OLTP databases (Cache/IDMS/Oracle/SQL) with

25,000 or more concurrent user, time-sensitive batch jobs with financial penalties for late completion and some virtualized platforms.

Minimum IO/sec - The SPC-1 minimum benchmark as identified in this standard provides for a independent and objective measuring tool with regards to IOPS (Input/Output operations per second) for which all potential SAN Solutions can be gauged. Specific test include OLTP, database operations and mail server implementations. Specifically SPC-1 is defined by www.storageperformance.com as "a single workload designed to demonstrate the performance of a storage subsystem while performing the typical functions of business critical applications. Those applications are characterized by predominately random I/O operations and require both queries as well as update operations". **The specific benchmark value was determined based on analysis of major vendor SPC benchmark submissions.**

Minimum Throughput - The SPC-2 minimum benchmark as identified in this standard provides for an independent and objective measuring tool with regards to MBPS (megabits per second) transfer rates for which all potential SAN Solutions can be gauged. Specific tests include large file processing, large database queries and video on demand (VOD). Specifically SPC-2 is defined by www.storageperformance.com as "three distinct workloads designed to demonstrate the performance of a storage subsystem during the execution of business critical applications that require the large-scale, sequential movement of data. Those applications are characterized predominately by large I/Os organized into one or more concurrent sequential patterns. A description of each of the three SPC-2 workloads is listed below as well as examples of applications characterized by each workload". **The specific benchmark value was determined based on analysis of major vendor SPC benchmark submissions.**

Storage unit uptime- In normal operation, the subsystem should not require more than five minutes interruption in a year for software upgrade or component replacement. Uptime is all connected hosts able to continue processing data. Additional Information can be gathered at http://www.uptimeinstitute.org.

Universal Device ID value (UDID) – In OpenVMS hosts must have a unique unit device identifier (UDID) for each accessible disk volume. To enable this, the subsystem must enable control over UDID assignment so that different disk arrays will not present the same UDID to the OpenVMS host.

Redundancy – Failure of a single component will not stop storage system operation in any capacity. Fully redundant storage systems are critical to the continuing processing and to maintain system stability.

FC – Host to Storage Connectivity – Storage subsystem must have multiple 4 Gb/second connectivity. An 8/GB connection is highly desirable.

iSCSI – Hosts to Storage Connectivity - For interoperability the SAN Solution that is procured must provide current iSCSI capabilities of 1GB current connectivity and the ability to upgrade to future higher speed connectivity. Additionally, Link Aggregation with dual NICS support is required.

SCSI Initiators (host connections) – a SCSI initiator is the host-side endpoint of a SCSI session. Every redundant host connection requires two SCSI initiators.

Replication – Replication is typically a software function, but hardware must support replication

LUN creation – The ability to create LUN's 'on the fly' without outage to the system and without disruption to the host systems.

LUN Expansion – Ability to add space to a LUN without rewriting data on that LUN.

Storage provisioning – Commonly called "thin provisioning". Thin provisioning is typically a software function, but hardware must support it.

Tiering capability - Manually or automatic policies to move inactive data to lower tier of storage, either in same or other frame. Tiering is typically a software function, but hardware must support it.

Resource partitioning capability – The ability to dedicate cache, ports or other subsystem resources to groups of LUNs or hosts.

Dynamic Tuning - The ability to create or update cache, ports or other subsystem resources to groups of LUNs or hosts while the system is serving I/O requests.

Backend Storage Virtualization – As the storage system will potentially be one of many with a heterogeneous data canter the capable to connect other backend storage devices from various storage vendors.

Snapshots – Snapshots are typically a software function, but hardware must support data snapshots (copy on write)

Clones – LUN cloning is typically a software function, but hardware must support data clone (full copies)

Storage device scale up capability – Upgrade controllers, cache or drives within same cabinets/footprint. Add controllers, cache, cabinets or drives without interrupting service or data migration.

Supported Disk type - As a minimum the SAN solution will provide the ability to utilize and support Fiber Channel drives, SATA drives and any near horizon drive technology (i.e. Solid State Drives) within the same SAN system.

Return disk option - As part of the support contract any failed disk within the SAN device or accompanying management servers will not be returned to the vendor. They will be maintained, secured and destroyed in accordance with applicable VA regulations with regards to data destruction.

Interoperability - Industry standards - for consistency and to ensure that the SAN Solution provided meets the criteria set forth by both Industry Standards and the VA Standard a baseline of specifications are needed. These specifications are best indicated by the Storage Management Initiative Specification (SMI-S) which was developed by leading storage equipment and software providers.

Firmware and microcode upgrade or updates - The capabilities to perform firmware and microcode updates without interrupt to the operations of the SAN and hosts devices connected there to. This is to include, but not limited to, disk firmware, controller firmware, controller software, and internal SAN Fabric switches.

SAN boot support (minimum) - The ability to provide the operating system of a host server to boot directly from the SAN device without local server disks is required. Please see the Operating Systems as listed in VA Technical Reference Model.

Operating system compatibility (minimum) - Please see the Operating Systems as listed in VA Technical Reference Model (TRM). The current VA TRM will be provided by COTR during acquisition process

Applications compatibility (minimum) - Please see the Applications as listed in VA Technical Reference Model. The current VA TRM will be provided by COTR during acquisition process.

Redundant Array of Independent Disk (RAID) levels - Due to the varying needs and uses the SAN Solution will be required to support the capabilities of RAID1, RAID5 and RAID6 in the same storage subsystems and disk enclosure. While above is a minimum RAID levels additional RAID configuration support is desired.

RAID group size - The size limit for a RAID group must not exceed 7TB in order to obtain optimal performance. The size requirement for a RAID group is based on the ability to rebuild the RAID group following a disk failure. Based on a drive MTTF of 1,000,000 hours, a RAID-5 group larger than 7 TB has a high risk of not being able to successfully rebuild without an unrecoverable error (URE). The existence of 7 drives to a RAID set is optimal and is the recommend amount to be allocated to any given RAID drive set.

Power switches - In addition to being redundant all power switches and power plugs must be properly secured and encased to ensure that they cannot be accidentally tripped, unseated or create any situation where power will be disrupted to the devices they are providing power to.

Standardized layouts - The layout of the solution must be a consistent design that is in use at all datacenters that are keeping with VA standards. This approach allows for the redistribution of the equipment to different sites and the most efficient use of data center space.

Additional servers - SAN support is often managed via a dedicated server(s). These hosts must be supported by the same support contract and remote management. Additionally all host must adhere to all the VA security policies and procedures with relation to servers, must be FIPS140-2 compliant and have only VA approved software installed.

Role-based Access - The ability for the applicable support personnel to manage the SAN solution and support servers from an industry standard out of band management solution is required and critical. Due to the remote nature and decentralized nature of support personnel must be able to access the SAN and servers even while shutdown or during BIOS/POST operations.

Documentation - Documentation must be provided that is described in the standard that allows for the complete understanding of the solution that is implemented. The importance of this is to create a seamless handoff from the varying organizations that will be supporting the SAN solution.

EVALUATION FACTORS

Lowest Total Cost of Ownership (TCO) solution that meets the performance requirements is preferred. Components considered are small footprint, power consumption, cooling, Hardware, Software, license, Overhead cost of managing the devices, Ease of Management, Acquisition cost, Maintenance and deployment costs, storage capacity (such as number of data copies),Information Lifecycle Management(ILM) cost.

Workload – The use of industry standard tools and benchmarks to provide adequate levels of validation during the acquisition process is critical to ensure the system procured can handle the rigors and high demands set forth in this tier.

Minimum IO/sec - The threshold of 100,000 IOPS using this SPC-1 benchmark has been identified as the minimum to provide the needs of the VistA application.

Minimum Throughput -The threshold of 5,000MBPS using this SPC-2 benchmark has been identified as the minimum to provide the needs of the VistA application.

Storage unit uptime – REQUIRED as defined in the standard above for this Tier. This would be 5 nines which equates to 5.26 minutes per year.

Universal Device ID value (UDID) - Required **in** order to support all the Operating Systems that may utilize the procured storage subsystem.

Redundancy – REQUIRED Redundant components are needed to ensure the failure of one component of the storage system will not cause an outage.

FC – Hosts to Storage Connectivity – REQUIRED **4**/GB connections however 8/GB connections are highly desirable and requested.

iSCSI – Hosts to Storage Connectivity – REQUIRED with minimum current iSCSI capabilities of 1GB connectivity with 10GB preferred and or expandable to in future.

SCSI Initiators (host connections) – a SCSI initiator is the host-side endpoint of a SCSI session. Every redundant host connection requires two SCSI initiators. The greater the available space to be assigned (usable) the more initiators would be required. Suggest at least one SCSI initiator for every two drive slots or 256 minimum.

Replication – Storage subsystem must support asynchronous and synchronous HA and DR replication

LUN Creation – LUN creation is a must in the type of environment that this tiered solution will be placed.

LUN Expansion – REQUIRED

Storage provisioning – Function included in cost. Thin provisioning is typically a software function, but hardware must support it.

Tiering capability – Function included in cost. Thin provisioning is typically a software function, but hardware must support it. Array needs to support or include multiple drive types or if tiering will be between multiple storage subsystems of heterogeneous types.

Resource partitioning capability and **Dynamic Tuning –** These two items must work together to allow for the dedication and allocation of resources to critical host or processes at a given time or event. Whether these are done manually or automatically by the storage system is a function of one or both of these specifications.

Backend Storage Virtualization – Determination will need to be made as to the vendor, type and specific storage system that the storage system being evaluated will connect, communicate and function with.

Snapshots – Compare limits on number of snapshots that can be made of a primary storage LUN

Clones – Compare limits on number of snapshots that can be made of a primary storage LUN

Storage device scale up capability – REQUIRED Evaluate based on expandability of usable storage in TB

Supported Disk type - REQUIRED the supported disk type must be specified in all documentation as to the exact type, speed and capacity.

Return disk option - REQUIRED To be documented in the procurement that no failed disks will be returned to vendor or leave in the possession of the VA at all times until properly disposed.

Interoperability – Industry standards – REQUIRED the supporting documentation should be presented and validated during the acquisition process. These specifications are SMI-S v1.1 as described at: http://www.snia.org/forums/smi/tech_programs/smis_home/

Firmware and microcode upgrade or updates – REQUIRED the means at which the vendor's solution will accomplish this task needs to be documented and tested prior to acceptance of the solutions.

SAN boot support (minimum) - REQUIRED to support the operating systems listed are required within this document

Operating system compatibility (minimum) – At a minimum the supported solution will provide OS support for Windows based Operating System, Linux Based Operating System, UNIX based Operating System and OpenVMS Operating System. The current VA TRM will be provided by COTR during acquisition process.

Applications compatibility (minimum) – The current VA TRM will be provided by COTR during acquisition process.

Redundant Array of Independent Disk (RAID) levels should meet the current and future needs of the VA. While the current VistA "Production data" resides on mirrored RAID1 drives the ability to augment them with addition RAID types is important. Raid group sizing limitations of Terabytes and number of physical drives is needed and should be evaluated as part of the acquisition process.

RAID group size - The size limit for a RAID group must not exceed 7TB in order to obtain optimal performance. The total number of drives assigned to a particular RAID set must not exceed seven physical drives. This is to ensure the integrity of the RAID group.

Power switches - All power switches and power plugs must be properly secured and encased

Standardized layouts - Layout and plan design will need to be validated during the acquisition process

Additional servers - All additional servers should be identified during the procurement process and keep with the VA Server Standards.

Role-based Access - Refer to Server Standard, Section Class C Server

Documentation - Cost of documentation should be identified and included in the procurement process. Vendor shall provide electronic, three dimensional models of equipment proposed for use with CAD and visual design/planning applications.

IMPLEMENTATION GUIDANCE

Lowest Total Cost of Ownership (TCO) solution that meets the performance requirements is preferred.

Workload- The use of industry standard tools and benchmarks to provide adequate verifications levels during acceptance testing. Extreme workloads are typically not the entire data hosted by a particular server. For example, in the case of databases, logs and indexes typically require more performance than other data. Data may be more efficiently hosted on multiple platforms.

Minimum IO/sec – Include validation in acceptance testing

Minimum Throughput – Include validation in acceptance testing

Storage Unit Uptime – Include validation in acceptance testing

Universal Device ID value (UDID) – Include validation in acceptance testing

Redundancy – Include validation in acceptance testing**.** Component failure testing should occur prior to putting into production. This should include a planned failure of a single component to ensure the backup/ secondary component provides adequate coverage to verify no outage of the storage system.

FC - Hosts to Storage Connectivity – Recommend 8/GB Fibre Channel connections to host.

iSCSI - Hosts to Storage Connectivity – Include validation in acceptance testing

iSCSI Initiator (Host Connections) - Include validation in acceptance testing

Replication – Testing of the replication process should occur during acceptance testing.

LUN Creation - Testing and actual creation for production should occur during acceptance testing to provide validation.

LUN Expansion – Include validation in acceptance testing

Storage Provisioning – Include validation in acceptance testing

Tiering Capability – If software is in place and capabilities exist the testing of this function should be conducted from this tier to a lower (or higher) tier.

Resource partitioning capability – The testing and validation of isolating subsystem components to specific hosts and process are measured and the findings documented and verified.

Dynamic Tuning – Stress testing and high usage simulation is done to validate. Dynamic Tuning should work very closely with Resource partitioning capability requirement to provide adequate resources to meet the needs of the processes and hosts at any given time.

Backend Storage Virtualization – Connection too and testing of the interoperability of the system being implemented to that of existing systems must be conducted and validated.

Snapshots – Include validation in acceptance testing

Clones – Include validation in acceptance testing

Supported Disk type - Fibre Channel and iSCSI are needed at a minimum.

Return disk option - Not applicable other than being aware of if any disk failure during implementation.

Interoperability – Industry standards - The standards which are provided in the sections above must be adhered to and validated during the implementation phase using the common set of tools identified in the SMI-S v1.1.

Firmware and microcode upgrade or updates - The means this is achieved by the SAN Solution needs to be tested.

SAN boot support (minimum) – Test and implement during installation with validation in acceptance testing

Operating system compatibility (minimum) - Include validation in acceptance testing

Applications compatibility (minimum) - Include validation in acceptance testing

Redundant Array of Independent Disk (RAID) levels - Include validation in acceptance testing

RAID group size - Include validation in acceptance testing

Power switches - All power switches and power plugs must be properly secured and encased. This also includes the proper covering of any emergency cutoff switches.

Standardized layouts - Ensure that all layouts conform to VA Standard and are validated during installation.

Additional servers - Operating System and Applications must be VA Server Standard. The current VA TRM will be provided by COTR during acquisition process. Refer to Server Standard, Section Class C Server

Role-Based Access – Described and documented in the support contract.

Documentation - All documentation should be in the form in a standard form that can be used by all VA support staff (i.e. Word documents, pdf or Visio).

3.1.2 [MAINFRAME SUPPORT]

STANDARD

ID	Secondary Attribute	Specification
	Parallel Access Volume (PAV)	Ability to support/exploit Parallel Access Volume (PAV).
	FICON support	Minimum 8-Gbit/s FICON Channel ports. Ability to support additional ports in the same enclosure
	HiperPAV support	Ability to support HiperPAV. Dynamic capabilities associated with Parallel Access Volumes.
	SMF support	Support SMF – Must have compatibility with this activity log recording feature
	Emulation types	Must be able to emulate 3390 based count key data devices.
	Solid State devices (SSD) support on Mainframe	Must be able to support solid state devices on Mainframe. Tools are needed to analyze mainframe data for SSD exploitation.
	Dynamic Channel Reconfiguration support	Must be able to support Dynamic Channel Reconfiguration.
	MIDAW support	Must be able to support MIDAW facility
	Priority I/O Queuing	Must be able to support Priority I/O Queuing

EXPLANATION OF STANDARD

EVALUATION FACTORS

-

IMPLEMENTATION GUIDANCE

3.1.3 [STORAGE MANAGEMENT SOFTWARE]

STANDARD

ID	Secondary Attribute	Specification
	Enterprise license not based on capacity	Software licenses provided must be perpetual with a five-year support and update subscription, with all licenses and rights transferred to the Government at the time the installation is completed. Licenses must be transferable without limitation and provisioned as a VA enterprise license, without additional storage allocation-based charges, such as per GB or TB.
	Interoperability	Management software must be listed as a Storage Networking Industry Association (SNIA) SMI-S 1.1 conforming client. (http://www.snia.org/forums/smi/tech_programs/ctp/smi_conform/smi_client/smi_client_definitions.
	Storage Reporting	Storage reporting components suitable for use in a fee for service, chargeback environment. Automated reports of storage allocations must be capable of being generated by non-IT staff. Must support ODBC and/or JDBC connectivity.
	Automated tools for LUN provisioning	The software should have automated tools to provision a large number of Disk Groups and LUNs. Similarly, an automated solution should be provided to configure hosts with large numbers of logical disks.
	Proactive monitoring and remote notification	The management tool must be capable of proactive monitoring and remote notification of system and application health. Must support ODBC and/or JDBC connectivity.
	Single storage management console	Storage hardware must be manageable from a single storage management application and with the capability of automatic discovery of equipment connected to the SAN.
	Additional servers	Refer to Server Standard, Section Class C Server
	Management server security	Refer to Server Standard, Section Class C Server
	Data snapshot (local)	License and annual maintenance (5 years) as required for software to support array-based point-in-time data images suitable for use for administrative tasks such as online backup & testing with no impact to source data and minimal additional space requirements.

	Performance analysis	Performance management software to monitor, analyze and report on all solution components (i.e. from host to fabric to storage). This includes storage subsystems, software operations, SAN infrastructure, replication and telecommunications. Software should be able to identify and analyze response time, and other relevant metrics to enable identification and resolution of potential bottlenecks. The tool must support OpenVMS client operating system. All management software must be ODBC and/or JDBC connectivity.
	Storage Capacity planning	The software must be able to analyze current capacity and forecasts future system requirements. The software should be able to collect component data to project future usage of the storage system.
	Local copy	License and annual maintenance (5 years) as required for software to support local array-array LUN copy/replication.
	Consistent design	All software should use identical components where possible to facilitate common updates across the solution.

EXPLANATION OF STANDARD

Enterprise license not based on capacity – to include 5 years of support as required for enterprise SAN Management application. Licenses must be transferable without limitation and provisioned as a VA enterprise license, without additional storage allocation-based charges, such as per GB or TB.

Interoperability - Management software must be listed as a Storage Networking Industry Association (SNIA) SMI-S 1.1 conforming client.
(http://www.snia.org/forums/smi/tech_programs/ctp/smi_conform/smi_client/smi_client_definitions

Storage Reporting – Access level reporting with the ability to generate reports by non-IT staff.

Automated tools for LUN provisioning - a single, intelligent interface that allows you to provision storage systems and fabric switches from end-to-end. The software should have automated tools to provision a large number of Disk Groups and LUNs along with the ability to configure hosts with large numbers of logical disks.

Proactive monitoring and remote notification - Storage Management software must be capable of monitoring and remote notification in the event of an alert, failure or the inability of the system to meet the customer's SLA's. Provisioning actions to trigger events, SNMP traps, and policies for notification. Ability to send email or custom scripts or programs for notification.

Single Storage Management console – Storage hardware must be manageable from a single storage management application.

Data snapshot (local) - License and annual maintenance (5 years) as required for software to support array-based point-in-time data images suitable for use for administrative tasks such as online backup & testing with no impact to source data and minimal additional space requirements.

Performance analysis – Storage management software to monitor, analyze and report on all solution components (i.e. from host to fabric to storage). This includes storage subsystems, software operations, SAN infrastructure, replication and telecommunications. Software should be able to identify and analyze response time, and other relevant metrics to enable identification and resolution of potential bottlenecks.

Storage Capacity planning - The software must be able to analyze current capacity and forecasts future system requirements. The software should be able to collect component data to project future usage of the storage system.

Local copy - License and annual maintenance (5 years) as required for software to support local array-array LUN copy/replication.

Consistent Design – All software should use identical components where possible to facilitate common updates across the solution.

EVALUATION FACTORS

- Enterprise Level Storage Management software
- Ability to manage multiple devices
- Enterprise License w/5years annual maintenance
- Storage Management Reporting
- Performance Monitoring
- Single Storage management console
- Ability to Manage events and policies

IMPLEMENTATION GUIDANCE

Implementation should include all optional software needed to meet the requirements listed above. Licensing and maintenance terms should the Hardware/Software Technical Support sections of this document. Professional implementation services should be included along with “classroom” training for support staff as outlined in the Training sections of this document.

3.1.4 [HARDWARE/SOFTWARE TECHNICAL SUPPORT]

STANDARD

ID	Secondary Attribute	Specification
	Support procedures	Documented support/escalation procedure for all components of the solution.
	Support Availability	Software support required 24x7x365 for all software provided in the solution. License and annual maintenance 3 years with 2 extension years.
		Hardware Maintenance/Support 5 yr, 24x7x365. For issue impacting production operation, Tier2 or greater phone support response should be available within the first hour and less than 4 hours response for Engineer to bring parts onsite.
	License transfer	Licenses can be transferred without limitation within the Department of Veterans Affairs.
	OEM resources	Direct access to on-line OEM vendor support incident information and tracking.
	Support Interface	All VA datacenters must have access to incident information and tracking for all VA datacenters.
	Disruptive patches	Describe any type of updates/patch that would require a hosted service outage of the solution.
	SLAs	Documented Service Level Agreements (SLAs) for support requests.
	Professional services	Include cost of any professional services for services that must be completed by the vendor.

EXPLANATION OF STANDARD

Support procedures – A documented (digital & printed) set of instructions and escalation procedures to include updated contact information for the appropriate point of contact while troubleshooting problems. This will be a living document and as such digital copies should have supplements/replacements provided quarterly to ensure the most up to date procedures are available for the customer.

A concisely documented set of procedures is essential for communication between the customer and the support staff, allowing for all parties to know when priority escalation occurs, how it occurs, and the proper path for the expedited resolution.

Support Availability – Due to the criticality of these systems, full round the clock support is essential for a minimum of the first year, with options available to extend for the following four years allowing for a total of five years. For issue impacting production operation, Tier2 or greater phone support response should be available within the first hour and less than 4 hours response for Engineer to bring parts onsite.

License transfer – All pertinent licenses must be capable of being transferred between various VA sites and cannot be restricted by location. Due to the nature of the OI&T structure for the VA licenses must be capable of being transferred within the various physical locations without restriction.

OEM resources – Direct communication paths to the knowledge experts of a product is key for fast response and ensuring the systems remain operational at the levels needed. Being required to go through middlemen in efforts to funnel trouble calls is not suitable to the nature of these systems.

Speaking directly with the product expert allows for potential miscommunication errors to be avoided. Being able to go directly to the appropriate level of tier knowledge on a failure is essential for ensuring that the problem is communicated correctly and quickly the best support engineer that can assist the customer.

Support interface – Due to many VA experts working across various regions and areas it is vital for all site's to be able to access VA wide information for troubleshooting and sharing of information.

VA I.T. support is organized through a central Office of Information Technology and is required to assist each various region/area as needed. Support contact and information should not be limited to a locality and must allow for access across the VA areas.

Disruptive patches – Ideally updates/patches will be able to be implemented with 0% system downtime. Any operations that would require a system outage needs to be documented and provided for review.

VA standards require that all disruptions be documented, submitted, and tracked to resolution. Known procedures that require disruption of service need to be documented and said documentation made available. Support engineers will need to work with VA staff to ensure that the required procedures for disruptions are followed.

SLAs - Documented Service Line Agreements (SLAs) for support request will be provided and the Vendor will ensure that there is no confusion between VA staff and Vendor on expectations.

Professional services – Provide a full disclosure of vendor specific services that must be provided by the vendor only. I.E. Some storage systems require a vendor engineer to flash firmware or similar upgrades and do not allow the customer to perform such actions.

VA standards require that outside contractors be escorted and/or evaluated for security requirements. All expected procedures that require vendor services need to be provided and a list of potential engineers that will be onsite updated as needed to ensure the engineer can gain access.

EVALUATION FACTORS

- Quality of documentation to include ease of finding information, extent of informative data, and usability in regards to trouble shooting and technical support will be considered.
- Direct phone contact for immediate escalation of troubleshooting over email, web interface, or other "automated" trouble shooting requests will be preferred.
- While direct access to product experts are needed, having a support engineer/contact to supervise and ensure that all experts are moving forward with the end goal of problem expedient problem resolution is preferred.
- Central/Single Interface for multiple sites to track VA related problems will be preferred.
- Minimum amount of scheduled downtime for patching/updating and supporting evidence for such is preferred.
- Path of communication for VA to suggest improvements and see improvements implemented is beneficial.
- Forums or other user group discussion areas are beneficial.
- Lower on-site response time is beneficial.
- Lower initial "engineer level" contact response time is beneficial.
- Lower time-to-repair is beneficial.
- Vendor-supplied components stocked as spares near, or at, facility is beneficial.
- Penalty clauses for vendor not meeting support contract provides is beneficial.

IMPLEMENTATION GUIDANCE

Coordination with initial VA staff for knowledge transfer and verified understanding is important. Continuing contact with VA staff to ensure support procedures are viable and procedures in place for VA input to improve support/product is essential.

3.1.5 [HARDWARE/SOFTWARE INSTALLATION]

STANDARD

ID	Secondary Attribute	Specification
	Installation	Provide hardware/software installation, including initial configuration, Storage Area Network configuration & knowledge transfer.
	Pre-configuration	Rack mount and configure the solution (including servers and storage where possible) prior to shipping it to the VA. This minimizes the on-site installation time as well as the number of crates and boxes that must be received and tracked by VA.
	Onsite impact	All on-site activities must be conducted in such a manner as to minimize the impact to normal information systems operations.
	Necessary software/hardware	Provide all necessary hardware and software, including all necessary cables and mounting hardware to make the Solution operational, except government-furnished property (GFP) referenced in GFP section.
	Delivery	Provide inside delivery, installation and insurance of all equipment to VA datacenters. The VA does not accept delivery of the equipment until acceptance testing is passed at all VA datacenters.
	Trash	Remove all trash associated with shipping, delivery and installation.
	OS installation and security	Refer to Server Standard, Section Class C Server

EXPLANATION OF STANDARD

Installation - Provide planning, configuration and tentative schedule for the initial installation. This planning should involve collaborating with customer technical personnel to insure any and all critical elements and requirements regarding the environment are communicated. This process is envisioned as a collaborative effort between the vendor and customer with the end result being an installation that is 100 percent complete, functional and fully documented and the customer understanding everything needed to operate and maintain the system. This also includes demonstrating the steps necessary to backup and restore the system to a fully functional state. This entire process is to be conducted in such a manner as to minimize the impact to normal information systems operation.

Pre-configuration - To shorten the installation process and better utilize the time vendor personnel are on-site it is required pre-racking and pre-configuring the solution as much as possible prior to delivery. This includes working with customer personnel to develop any custom software images and preload the images prior to shipping.

Restorable images – In addition to having hardware preloaded with software a process must be in place to have restorable images for these systems as a backup to needing to overwrite/restore an existing image during install. Custom DVD's, portable storage, etc… are all viable options to having the image onsite for quick access and use.

Onsite impact – Minimal impact on the site facility is required. Efforts will be taken by the Vendor to ensure that the prep, assembly, install, and testing of the Solution will be done in a professional manner with minimal impact upon local site. Concern in regards to trash, path blockage, unsecured equipment, excessive levels of noise, etc… should be considered and action taken accordingly.

Necessary software/hardware – Aside from government-furnished property (GFP) referenced in the GFP section, all software and hardware required to make the Solution operational will be provided by the Vendor. This is to include but not limited to: cables, mounting brackets, screws, install software, testing equipment, etc…

Delivery – The Vendor will take responsibility of ensuring that all materials are delivered into the facility install location and the materials will remain the responsibility of the Vendor until acceptance testing is passed at all VA datacenters.

Trash – The Vendor will take responsibility of the removal of all trash from the facility, including but not limited to: boxes, packing materials, plastic bags, ties, etc…

OS installation and security – Following existing documentation provide by the VA Platform Server Team ensure all Operating systems and Security applications are installed accordingly.

EVALUATION FACTORS

- It is considered beneficial if the vendor can detail a delivery, installation and configuration plan for the equipment the vendor is proposing.
- Any demonstration that equipment can be pre-racked, pre-configured or pre-imaged is considered beneficial
- Verification that images can be restored onsite instead of remotely for install purposes is preferred.
- A basic plan to show minimal impact during installation and setup with certified technicians to follow this plan is preferred. Vendor hiring lowest cost "IT Talent" is not preferred.
- Checklists of hardware and software installation needs and verified availability of these is beneficial.

IMPLEMENTATION GUIDANCE

As much Vendor/VA staff preinstall communication to ensure full understanding is recommended.

Vendor verification of hardware fitting and requirements prior to install is required. Finding out at install that a piece of equipment does not fit or does not have all the install equipment is not acceptable.

All documentation, software, and hardware required for installation and operation of the Solution as well as training materials need to be onsite and verified for installation.

3.1.6 [TRAINING]

STANDARD

ID	Secondary Attribute	Specification
5	Training Length	Provide equivalent of one hour of certified vendor classroom training for every TB of raw disk provided.
	Knowledge transfer	Work with VA staff as activities occur to ensure that VA can assume operational responsibility for the delivered solution.
	Documentation	Provide electronic copies of all materials, manuals, worksheets, etc. used in the delivery of the solution.

EXPLANATION OF STANDARD

Training Length – An initial complete training for VA staff is important for this project to succeed. An equivalent of one hour of certified vendor classroom training for every TB of raw disk provided, or more if the vendor believes this is needed.

VA support staff must have a level of trained knowledge provided to allow them to operate at a high level of expertise for day to day operations and standard problem resolution.

Knowledge transfer – While classroom training is important for the understanding of principles and procedures, actual knowledge transfer in regards to the implemented packages, how they work in the VA environment and potential improvement that may be available or upcoming is required.

Documentation – Initially all documentation for training, materials, worksheets, etc… for the initial installation must be provided in electronic format to ensure standard knowledge for all VA staff. As the product is changed and improved future training and documentation will also need to be provided.

Training documentation must be as complete as possible to allow for new VA staff to be able to understand and work with the vendor product.

EVALUATION FACTORS

- Vendor specific training that is oriented towards certification or “engineer” level training that is pertinent to properly managing and troubleshooting the product is preferred.
- Additional time/effort spent working with VA staff to ensure that the VA environment is optimized and meeting VA expectations is beneficial.
- When directly training VA staff printed as well as digital materials is beneficial to allow full potential of learning from staff.
- User forums for exchange of ideas and knowledge are preferred.

IMPLEMENTATION GUIDANCE

Any implementation that requires a strong base of knowledge for VA staff needs to have a planned training event set in place prior to installation to allow for full VA understanding and best potential for project implementation. While this training should be prior to installation it must not be so far in advance that newly learned skills/knowledge will become stale/obsolete by installation time.

In addition any installation that will occur near a time of a new patch or revision needs to ensure that the new knowledge is provided with the training.

3.2 [TIER 2 STORAGE SERVICE]

3.2.1 [STORAGE SUBSYSTEM HARDWARE (HW)]

STANDARD

ID	Secondary Attribute	Specification
	Workload	Capable to support Medium Performance such as Exchange Server, SQL Server, Virtual servers and generalized web servers with 25,000 or less concurrent users Workload.
	Minimum IO/sec	50,000 SPC-1 IOPS™ as measured by SPC-1 benchmark (http://www.storageperformance.org/results/)
	Minimum Throughput	1,000 SPC-2 MBPS™ as measured by SPC-2 benchmark (http://www.storageperformance.org/results/)
	Storage unit uptime	4'9s uptime.
	Universal Device ID value (UDID)	Changeable LUN UDID value is required.
	Redundancy	Fully redundant power supplies, cooling fans, component controllers, and others. All controllers within a single module will automatically fail over and load balance with one another. Controller module will support a minimum of two controllers.
	FC - Hosts to Storage Connectivity	Storage subsystems must support minimum four 4-Gbit/s Fiber Channel ports. Ability to support ports expansion to meet Tier 1 performance requirements in the same unit(s).
		Minimum two redundant multi-path connections from Host to Storage device. The Host connectivity throughput and performance will not be degraded even if 50% of the Host connectivity is lost.
	iSCSI - Hosts to Storage Connectivity	Storage subsystems must support minimum 1 Gb Ethernet connectivity with link aggregation. 10 Gb Ethernet support is preferred. Controller module will support a minimum of four Ethernet ports. Ability to support ports expansion in the same unit(s). Support Jumbo frame and LACP protocol.
		Minimum two redundant multi-path connections from Host to Storage device. The Host connectivity throughput and performance will not be degraded even if 50% of the Host connectivity is lost.

	SCSI Initiator (Host Connections)	Support a minimum of 256
	Replication	Capable of synchronous and asynchronous replication with write order fidelity.
	LUN creation	Ability to create LUN across all spindles.
	LUN Expansion	Dynamic LUN expansion is required.
	Storage provisioning	Capable of over-provisioning or Over-allocation storage capacity that allows hosts to view more storage capacity than has been physically reserved on the storage array itself
	Tiering capability	Using policies to move inactive data to lower tier of storage
	Deduplication	Minimum support post process deduplication.
	Snapshots	Capable of creating point in time delta snapshot Capable of creating space efficient snapshots on an as needed basis versus snapshot space reservation
	Clones	Capable of creating point in time delta clone Capable of creating space efficient clones on an as needed basis versus snapshot space reservation. Immediate access to clones before it is completed.
	Storage device scale up capability	Ability to upgrade controller/controller module on storage device without forklift upgrade.
		Adding or upgrading storage subsystem components adhering to the required storage device uptime requirement and no data migration
	Supported Disk type	Ability to support sufficient disk drive technologies to meet Tier 2 performance requirements.
	Return disk option	Non-return disk option is required
	Interoperability - Industry standards	Each storage subsystem must provide Storage Management Initiative Specification (SMI-S) 1.1 conforming provider (http://www.snia.org/ctp/conformingproviders)
	Firmware and microcode upgrade or updates	Completely non-disruptive to operations firmware and microcode upgrade or updates for all components with zero downtime are required.
	Boot from SAN	Storage subsystem will support boot from San.

	Operating system and file system compatibility	Must support operating systems and their associated file systems as listed in the TRM.
	Applications compatibility (minimum)	Applications listed by VA Technical Reference Model (TRM) for enterprise deployment.
	Redundant Array of Independent Disk (RAID) levels	Minimum support for RAID 0+1/10/5/6 in same subsystems.
	RAID group size	Vendor offering must be able to meet storage capacity without exceeding 7 TB RAID group size and without exceeding 7 data drives.
	Power switches	Master power switches must be covered to prevent inadvertent activation.
	Standardized layouts	Components must be mounted in standardized configurations for all VA installations.
	Additional servers	Refer to Server Standard, Section Class C Server
	Role-based access	Solution must include security configurations that support role-based access required to limit functions during normal and COOP operation.
	Documentation	Provide detail design solution documents and drawings. All design methods and calculations to achieve the performance requirements must be clearly stated in the document. All assumptions if any must be included in the design document

EXPLANATION OF STANDARD

Workload – The storage system must be able to handle the amount of data and transactions that accompany large shared enterprise level applications with high amounts of transactions and large amounts of I/O. Capable of supporting medium and high performance workloads such as OLTP databases (Cache/IDMS/Oracle/SQL) with less than 25,000 concurrent users, VistA, Microsoft Exchange, general web and application servers and virtualized platforms.

Minimum IO/sec - The SPC-1 minimum benchmark as identified in this standard provides for a independent and objective measuring tool with regards to IOPS (Input/Output operations per second) for which all potential SAN Solutions can be gauged. Specific test include OLTP, database operations and mail server implementations. Specifically SPC-1 is defined by www.storageperformance.com as "a single workload designed to demonstrate the performance of a storage subsystem while performing the typical functions of business critical applications. Those applications are characterized by predominately random I/O operations and require both queries as well as update operations". **The specific benchmark value was determined based on analysis of major vendor SPC benchmark submissions.**

Minimum Throughput - The SPC-2 minimum benchmark as identified in this standard provides for an independent and objective measuring tool with regards to MBPS (megabits per second) transfer rates for which all potential SAN Solutions can be gauged. Specific tests include large file processing, large database queries and video on demand (VOD). Specifically SPC-2 is defined by www.storageperformance.com as "three distinct workloads designed to demonstrate the performance of a storage subsystem during the execution of business critical applications that require the large-scale, sequential movement of data. Those applications are characterized predominately by large I/Os organized into one or more concurrent sequential patterns. A description of each of the three SPC-2 workloads is listed below as well as examples of applications characterized by each workload". **The specific benchmark value was determined based on analysis of major vendor SPC benchmark submissions.**

Storage unit uptime- In normal operation, the subsystem should not require more than fifty two minutes interruption in a year for software upgrade or component replacement. Uptime is all connected hosts able to continue processing data. Additional Information can be gathered at http://www.uptimeinstitute.org.

Universal Device ID value (UDID) – In OpenVMS hosts must have a unique unit device identifier (UDID) for each accessible disk volume. To enable this, the subsystem must enable control over UDID assignment so that different disk arrays will not present the same UDID to the OpenVMS host.

Redundancy – Failure of a single component will not stop storage system operation in any capacity. Fully redundant storage systems are critical to the continuing processing and to maintain system stability.

FC – Host to Storage Connectivity – Storage subsystem must have multiple 4 Gb/second connectivity. An 8/GB connection is highly desirable.

iSCSI – Hosts to Storage Connectivity - For interoperability the SAN Solution that is procured must provide current iSCSI capabilities of 1GB current connectivity and the ability to upgrade to future higher speed connectivity. Additionally, Link Aggregation with dual NICS support is required.

SCSI Initiators (host connections) – a SCSI initiator is the host-side endpoint of a SCSI session. Every redundant host connection requires two SCSI initiators.

Replication – Replication is typically a software function, but hardware must support replication

LUN creation – The ability to create LUN's 'on the fly' without outage to the system and without disruption to the host systems.

LUN Expansion – Ability to add space to a LUN without rewriting data on that LUN.

Storage provisioning – Commonly called "thin provisioning". Thin provisioning is typically a software function, but hardware must support it.

Tiering capability - Manually or automatic policies to move inactive data to lower tier of storage, either in same or other frame. Tiering is typically a software function, but hardware must support it.

Deduplication – Data Deduplication is a technology strives to reduce the amount of duplicate data being backed up and then stored. The technologies identify and eliminate common data in and across backup streams. By eliminating the common objects, the resulting storage requirement will be reduced.

Global deduplication comes into play when you have multiple deduplication devices. With multiple deduplication devices nodes, when data that is seen before by one node is sent to a second node, the second node knows that data has already been stored and it will not be stored for a second time.

Snapshots – Snapshots are typically a software function, but hardware must support data snapshots (copy on write)

Clones – LUN cloning is typically a software function, but hardware must support data clone (full copies)

Storage device scale up capability – Upgrade controllers, cache or drives within same cabinets/footprint. Add controllers, cache, cabinets or drives without interrupting service or data migration.

Supported Disk type - As a minimum the SAN solution will provide the ability to utilize and support Fibre Channel drives, SATA drives and any near horizon drive technology (i.e. Solid State Drives) within the same SAN system.

Return disk option - As part of the support contract any failed disk within the SAN device or accompanying management servers will not be returned to the vendor. They will be maintained, secured and destroyed in accordance with applicable VA regulations with regards to data destruction.

Interoperability - Industry standards - for consistency and to ensure that the SAN Solution provided meets the criteria set forth by both Industry Standards and the VA Standard a baseline of specifications are needed. These specifications are best indicated by the Storage Management Initiative Specification (SMI-S) which was developed by leading storage equipment and software providers.

Firmware and microcode upgrade or updates - The capabilities to perform firmware and microcode updates without interrupt to the operations of the SAN and hosts devices connected there to. This is to include, but not limited to, disk firmware, controller firmware, controller software, and internal SAN Fabric switches.

SAN boot support (minimum) - The ability to provide the operating system of a host server to boot directly from the SAN device without local server disks is required. Please see the Operating Systems as listed in VA Technical Reference Model.

Operating system compatibility (minimum) - Please see the Operating Systems as listed in VA Technical Reference Model (TRM). The current VA TRM will be provided by COTR during acquisition process

Applications compatibility (minimum) - Please see the Applications as listed in VA Technical Reference Model. The current VA TRM will be provided by COTR during acquisition process.

Redundant Array of Independent Disk (RAID) levels - Due to the varying needs and uses the SAN Solution will be required to support the capabilities of RAID1, RAID5 and RAID6 in the same storage subsystems and disk enclosure. While above is a minimum RAID levels additional RAID configuration support is desired.

RAID group size - The size limit for a RAID group must not exceed 7TB in order to obtain optimal performance. The size requirement for a RAID group is based on the ability to rebuild the RAID group following a disk failure. Based on a drive MTTF of 1,000,000 hours, a RAID-5 group larger than 7 TB has a high risk of not being able to successfully rebuild without an unrecoverable error (URE). The existence of 7 drives to a RAID set is optimal and is the recommend amount to be allocated to any given RAID drive set.

Power switches - In addition to being redundant all power switches and power plugs must be properly secured and encased to ensure that they cannot be accidentally tripped, unseated or create any situation where power will be disrupted to the devices they are providing power to.

Standardized layouts - The layout of the solution must be a consistent design that is in use at all datacenters that are keeping with VA standards. This approach allows for the redistribution of the equipment to different sites and the most efficient use of data center space.

Additional servers - SAN support is often managed via a dedicated server(s). These hosts must be supported by the same support contract and remote management. Additionally all host must adhere to all the VA security policies and procedures with relation to servers, must be FIPS140-2 compliant and have only VA approved software installed.

Role-based Access - The ability for the applicable support personnel to manage the SAN solution and support servers from an industry standard out of band management solution is required and critical. Due to the remote nature and decentralized nature of support personnel must be able to access the SAN and servers even while shutdown or during BIOS/POST operations.

Documentation - Documentation must be provided that is described in the standard that allows for the complete understanding of the solution that is implemented. The importance of this is to create a seamless handoff from the varying organizations that will be supporting the SAN solution.

EVALUATION FACTORS

Lowest Total Cost of Ownership (TCO) solution that meets the performance requirements is preferred. Components considered are small footprint, power consumption, cooling, Hardware, Software, license, Overhead cost of managing the devices, Ease of Management, Acquisition cost, Maintenance and deployment costs, storage capacity (such as number of data copies),Information Lifecycle Management(ILM) cost.

Workload – The use of industry standard tools and benchmarks to provide adequate levels of validation during the acquisition process is critical to ensure the system procured can handle the rigors and high demands set forth in this tier.

Minimum IO/sec - The threshold of 50,000 IOPS using this SPC-1 benchmark has been identified as the minimum to provide the needs of the VistA application.

Minimum Throughput -The threshold of 1,000MBPS using this SPC-2 benchmark has been identified as the minimum to provide the needs of the VistA application.

Storage unit uptime – REQUIRED as defined in the standard above for this Tier. This would be 4 nines which equates to 52.6 minutes per year.

Universal Device ID value (UDID) - Required **in** order to support all the Operating Systems that may utilize the procured storage subsystem.

Redundancy – REQUIRED Redundant components are needed to ensure the failure of one component of the storage system will not cause an outage.

FC – Hosts to Storage Connectivity – REQUIRED **4**/GB connections however 8/GB connections are highly desirable and requested.

iSCSI – Hosts to Storage Connectivity – REQUIRED with minimum current iSCSI capabilities of 1GB connectivity with 10GB preferred and or expandable to in future.

SCSI Initiators (host connections) – a SCSI initiator is the host-side endpoint of a SCSI session. Every redundant host connection requires two SCSI initiators. The greater the available space to be assigned (usable) the more initiators would be required. Suggest at least one SCSI initiator for every two drive slots or 256 minimum.

Replication – Storage subsystem must support asynchronous and synchronous HA and DR replication

LUN Creation – LUN creation is a must in the type of environment that this tiered solution will be placed.

LUN Expansion – REQUIRED

Storage provisioning – Function included in cost. Thin provisioning is typically a software function, but hardware must support it.

Tiering capability – Function included in cost. Thin provisioning is typically a software function, but hardware must support it. Array needs to support or include multiple drive types or if tiering will be between multiple storage subsystems of heterogeneous types.

Deduplication – Source, target, inline, or post process deduplication. The deduplication method used must not degrade overall application performance, storage performance, and will not reduce backup windows. Support Global deduplication is preferred.

Capable of perform both file-level, and block-level data deduplication is preferred.

Capable of perform both file-level and block-level data deduplication on primary storage is preferred.

Snapshots – Compare limits on number of snapshots that can be made of a primary storage LUN

Clones – Compare limits on number of snapshots that can be made of a primary storage LUN

Storage device scale up capability – REQUIRED Evaluate based on expandability of usable storage in TB

Supported Disk type - REQUIRED the supported disk type must be specified in all documentation as to the exact type, speed and capacity.

Return disk option - REQUIRED To be documented in the procurement that no failed disks will be returned to vendor or leave in the possession of the VA at all times until properly disposed.

Interoperability – Industry standards – REQUIRED the supporting documentation should be presented and validated during the acquisition process. These specifications are SMI-S v1.1 as described at: http://www.snia.org/forums/smi/tech_programs/smis_home/

Firmware and microcode upgrade or updates – REQUIRED the means at which the vendor's solution will accomplish this task needs to be documented and tested prior to acceptance of the solutions.

SAN boot support (minimum) - REQUIRED to support the operating systems listed are required within this document

Operating system compatibility (minimum) – At a minimum the supported solution will provide OS support for Windows based Operating System, Linux Based Operating System, UNIX based Operating System and OpenVMS Operating System. The current VA TRM will be provided by COTR during acquisition process.

Applications compatibility (minimum) – The current VA TRM will be provided by COTR during acquisition process.

Redundant Array of Independent Disk (RAID) levels should meet the current and future needs of the VA. While the current VistA "Production data" resides on mirrored RAID1 drives the ability to augment them with addition RAID types is important. Raid group sizing limitations of Terabytes and number of physical drives is needed and should be evaluated as part of the acquisition process.

RAID group size - The size limit for a RAID group must not exceed 7TB in order to obtain optimal performance. The total number of drives assigned to a particular RAID set must not exceed seven physical drives. This is to ensure the integrity of the RAID group.

Power switches - All power switches and power plugs must be properly secured and encased

Standardized layouts - Layout and plan design will need to be validated during the acquisition process

Additional servers - All additional servers should be identified during the procurement process and keep with the VA Server Standards.

Role-based Access - Refer to Server Standard, Section Class C Server

Documentation - Cost of documentation should be identified and included in the procurement process. Vendor shall provide electronic, three dimensional models of equipment proposed for use with CAD and visual design/planning applications.

IMPLEMENTATION GUIDANCE

Lowest Total Cost of Ownership (TCO) solution that meets the performance requirements is preferred.

Workload- The use of industry standard tools and benchmarks to provide adequate verifications levels during acceptance testing

Minimum IO/sec – Include validation in acceptance testing

Minimum Throughput – Include validation in acceptance testing

Storage Unit Uptime – Include validation in acceptance testing

Universal Device ID value (UDID) – Include validation in acceptance testing

Redundancy – Include validation in acceptance testing**.** Component failure testing should occur prior to putting into production. This should include a planned failure of a single component to ensure the backup/ secondary component provides adequate coverage to verify no outage of the storage system.

FC - Hosts to Storage Connectivity – Recommend 8/GB Fibre Channel connections to host.

iSCSI - Hosts to Storage Connectivity – Include validation in acceptance testing

iSCSI Initiator (Host Connections) - Include validation in acceptance testing

Replication – Testing of the replication process should occur during acceptance testing.

LUN Creation - Testing and actual creation for production should occur during acceptance testing to provide validation.

LUN Expansion – Include validation in acceptance testing

Storage Provisioning – Include validation in acceptance testing

Tiering Capability – If software is in place and capabilities exist the testing of this function should be conducted from this tier to a lower (or higher) tier.

Deduplication – Must test and validate to ensure the deduplication method used does not degrade overall application performance, storage performance, and will not reduce backup windows. Test and validate to ensure Global deduplication only process on copy of data among sites.

Snapshots – Include validation in acceptance testing

Clones – Include validation in acceptance testing

Supported Disk type - Fibre Channel and iSCSI are needed at a minimum.

Return disk option - Not applicable other than being aware of if any disk failure during implementation.

Interoperability – Industry standards - The standards which are provided in the sections above must be adhered to and validated during the implementation phase using the common set of tools identified in the SMI-S v1.1.

Firmware and microcode upgrade or updates - The means this is achieved by the SAN Solution needs to be tested.

SAN boot support (minimum) – Test and implement during installation with validation in acceptance testing

Operating system compatibility (minimum) - Include validation in acceptance testing

Applications compatibility (minimum) - Include validation in acceptance testing

Redundant Array of Independent Disk (RAID) levels - Include validation in acceptance testing

RAID group size - Include validation in acceptance testing

Power switches - All power switches and power plugs must be properly secured and encased. This also includes the proper covering of any emergency cutoff switches.

Standardized layouts - Ensure that all layouts conform to VA Standard and are validated during installation.

Additional servers - Operating System and Applications must be VA Server Standard. The current VA TRM will be provided by COTR during acquisition process. Refer to Server Standard, Section Class C Server

Role-Based Access – Described and documented in the support contract.

Documentation - All documentation should be in the form in a standard form that can be used by all VA support staff (i.e. Word documents, pdf or Visio).

3.2.2 [STORAGE MANAGEMENT SOFTWARE]

STANDARD

ID	Secondary Attribute	Specification
	Enterprise license not based on capacity	Software licenses provided must be perpetual with a five-year support and update subscription, with all licenses and rights transferred to the Government at the time the installation is completed. Licenses must be transferable without limitation and provisioned as a VA enterprise license, without additional storage allocation-based charges, such as per GB or TB.
	Interoperability	Management software must be listed as a Storage Networking Industry Association (SNIA) SMI-S 1.1 conforming client. (http://www.snia.org/forums/smi/tech_programs/ctp/smi_conform/smi_client/smi_client_definitions.
	Storage Reporting	Storage reporting components suitable for use in a fee for service, chargeback environment. Automated reports of storage allocations must be capable of being generated by non-IT staff. Must support ODBC and/or JDBC connectivity.
	Automated tools for LUN provisioning	The software should have automated tools to provision a large number of Disk Groups and LUNs. Similarly, an automated solution should be provided to configure hosts with large numbers of logical disks.
	Proactive monitoring and remote notification	The management tool must be capable of proactive monitoring and remote notification of system and application health. Must support ODBC and/or JDBC connectivity.
	Single storage management console	Storage hardware must be manageable from a single storage management application and with the capability of automatic discovery of equipment connected to the SAN.
	Additional servers	Refer to Server Standard, Section Class C Server
	Management server security	Refer to Server Standard, Section Class C Server
	Data snapshot (local)	License and annual maintenance (5 years) as required for software to support array-based point-in-time data images suitable for use for administrative tasks such as online backup & testing with no impact to source data and minimal additional space requirements.

	Performance analysis	Performance management software to monitor, analyze and report on all solution components (i.e. from host to fabric to storage). This includes storage subsystems, software operations, SAN infrastructure, replication and telecommunications. Software should be able to identify and analyze response time, and other relevant metrics to enable identification and resolution of potential bottlenecks. The tool must support OpenVMS client operating system. All management software must be ODBC and/or JDBC connectivity.
	Storage Capacity planning	The software must be able to analyze current capacity and forecasts future system requirements. The software should be able to collect component data to project future usage of the storage system.
	Local copy	License and annual maintenance (5 years) as required for software to support local array-array LUN copy/replication.
	Consistent design	All software should use identical components where possible to facilitate common updates across the solution.

EXPLANATION OF STANDARD

Enterprise license not based on capacity – to include 5 years of support as required for enterprise SAN Management application. Licenses must be transferable without limitation and provisioned as a VA enterprise license, without additional storage allocation-based charges, such as per GB or TB.

Interoperability - Management software must be listed as a Storage Networking Industry Association (SNIA) SMI-S 1.1 conforming client.
(http://www.snia.org/forums/smi/tech_programs/ctp/smi_conform/smi_client/smi_client_definitions

Storage Reporting – Access level reporting with the ability to generate reports by non-IT staff.

Automated tools for LUN provisioning - a single, intelligent interface that allows you to provision storage systems and fabric switches from end-to-end. The software should have automated tools to provision a large number of Disk Groups and LUNs along with the ability to configure hosts with large numbers of logical disks.

Proactive monitoring and remote notification - Storage Management software must be capable of monitoring and remote notification in the event of an alert, failure or the inability of the system to meet the customer's SLA's. Provisioning actions to trigger events, SNMP traps, and policies for notification. Ability to send email or custom scripts or programs for notification.

Single Storage Management console – Storage hardware must be manageable from a single storage management application.

Data snapshot (local) - License and annual maintenance (5 years) as required for software to support array-based point-in-time data images suitable for use for administrative tasks such as online backup & testing with no impact to source data and minimal additional space requirements.

Performance analysis – Storage management software to monitor, analyze and report on all solution components (i.e. from host to fabric to storage). This includes storage subsystems, software operations, SAN infrastructure, replication and telecommunications. Software should be able to identify and analyze response time, and other relevant metrics to enable identification and resolution of potential bottlenecks.

Storage Capacity planning - The software must be able to analyze current capacity and forecasts future system requirements. The software should be able to collect component data to project future usage of the storage system.

Local copy - License and annual maintenance (5 years) as required for software to support local array-array LUN copy/replication.

Consistent Design – All software should use identical components where possible to facilitate common updates across the solution.

EVALUATION FACTORS

- Enterprise Level Storage Management software
- Ability to manage multiple devices
- Enterprise License w/5years annual maintenance
- Storage Management Reporting
- Performance Monitoring
- Single Storage management console
- Ability to Manage events and policies

IMPLEMENTATION GUIDANCE

Implementation should include all optional software needed to meet the requirements listed above. Licensing and maintenance terms should the Hardware/Software Technical Support sections of this document. Professional implementation services should be included along with “classroom” training for support staff as outlined in the Training sections of this document.

3.2.3 [HARDWARE/SOFTWARE TECHNICAL SUPPORT]

STANDARD

ID	Secondary Attribute	Specification
	Support procedures	Documented support/escalation procedure for all components of the solution.
	Support Availability	Software support required 24x7x365 for all software provided in the solution. License and annual maintenance 3 years with 2 extension years.
		Hardware Maintenance/Support 5 yr, 24x7x365, 4 hour response time is required.
	License transfer	Licenses can be transferred without limitation within the Department of Veterans Affairs.
	OEM resources	Direct access to on-line OEM vendor support incident information and tracking.
	Support Interface	All VA datacenters must have access to incident information and tracking for all VA datacenters.
	Disruptive patches	Describe any type of updates/patch that would require a hosted service outage of the solution.
	SLAs	Documented Service Level Agreements (SLAs) for support requests.
	Professional services	Include cost of any professional services for services that must be completed by the vendor.

EXPLANATION OF STANDARD

Support procedures – A documented (digital & printed) set of instructions and escalation procedures to include updated contact information for the appropriate point of contact while troubleshooting problems. This will be a living document and as such digital copies should have supplements/replacements provided quarterly to ensure the most up to date procedures are available for the customer.

A concisely documented set of procedures is essential for communication between the customer and the support staff, allowing for all parties to know when priority escalation occurs, how it occurs, and the proper path for the expedited resolution.

Support Availability – Due to the criticality of these systems, full round the clock support is essential for a minimum of the first year, with options available to extend for the following four years allowing for a total of five years. In addition a minimal 4 hour response time in regards to hardware maintenance is required.

License transfer – All pertinent licenses must be capable of being transferred between various VA sites and cannot be restricted by location. Due to the nature of the OI&T structure for the VA licenses must be capable of being transferred within the various physical locations without restriction.

OEM resources – Direct communication paths to the knowledge experts of a product is key for fast response and ensuring the systems remain operational at the levels needed. Being required to go through middlemen in efforts to funnel trouble calls is not suitable to the nature of these systems.

Speaking directly with the product expert allows for potential miscommunication errors to be avoided. Being able to go directly to the appropriate level of tier knowledge on a failure is essential for ensuring that the problem is communicated correctly and quickly the best support engineer that can assist the customer.

Support interface – Due to many VA experts working across various regions and areas it is vital for all site's to be able to access VA wide information for troubleshooting and sharing of information.

VA I.T. support is organized through a central Office of Information Technology and is required to assist each various region/area as needed. Support contact and information should not be limited to a locality and must allow for access across the VA areas.

Disruptive patches – Ideally updates/patches will be able to be implemented with 0% system downtime. Any operations that would require a system outage needs to be documented and provided for review.

VA standards require that all disruptions be documented, submitted, and tracked to resolution. Known procedures that require disruption of service need to be documented and said documentation made available. Support engineers will need to work with VA staff to ensure that the required procedures for disruptions are followed.

SLAs - Documented Service Line Agreements (SLAs) for support request will be provided and the Vendor will ensure that there is no confusion between VA staff and Vendor on expectations.

Professional services – Provide a full disclosure of vendor specific services that must be provided by the vendor only. I.E. Some storage systems require a vendor engineer to flash firmware or similar upgrades and do not allow the customer to perform such actions.

VA standards require that outside contractors be escorted and/or evaluated for security requirements. All expected procedures that require vendor services need to be provided and a list of potential engineers that will be onsite updated as needed to ensure the engineer can gain access.

EVALUATION FACTORS

- Quality of documentation to include ease of finding information, extent of informative data, and usability in regards to trouble shooting and technical support will be considered.

- Direct phone contact for immediate escalation of troubleshooting over email, web interface, or other "automated" trouble shooting requests will be preferred.
- While direct access to product experts are needed, having a support engineer/contact to supervise and ensure that all experts are moving forward with the end goal of problem expedient problem resolution is preferred.
- Central/Single Interface for multiple sites to track VA related problems will be preferred.
- Minimum amount of scheduled downtime for patching/updating and supporting evidence for such is preferred.
- Path of communication for VA to suggest improvements and see improvements implemented is beneficial.
- Forums or other user group discussion areas are beneficial.
- Lower on-site response time is beneficial.
- Lower initial "engineer level" contact response time is beneficial.
- Lower time-to-repair is beneficial.
- Vendor-supplied components stocked as spares near, or at, facility is beneficial.
- Penalty clauses for vendor not meeting support contract provides is beneficial.

IMPLEMENTATION GUIDANCE

Coordination with initial VA staff for knowledge transfer and verified understanding is important. Continuing contact with VA staff to ensure support procedures are viable and procedures in place for VA input to improve support/product is essential.

3.2.4 [HARDWARE/SOFTWARE INSTALLATION]

STANDARD

ID	Secondary Attribute	Specification
	Installation	Provide hardware/software installation, including initial configuration, Storage Area Network configuration & knowledge transfer.
	Pre-configuration	Rack mount and configure the solution (including servers and storage where possible) prior to shipping it to the VA. This minimizes the on-site installation time as well as the number of crates and boxes that must be received and tracked by VA.
	Onsite impact	All on-site activities must be conducted in such a manner as to minimize the impact to normal information systems operations.
	Necessary software/hardware	Provide all necessary hardware and software, including all necessary cables and mounting hardware to make the Solution operational, except government-furnished property (GFP) referenced in GFP section.
	Delivery	Provide inside delivery, installation and insurance of all equipment to VA datacenters. The VA does not accept delivery of the equipment until acceptance testing is passed at all VA datacenters.
	Trash	Remove all trash associated with shipping, delivery and installation.
	OS installation and security	Refer to Server Standard, Section Class C Server

EXPLANATION OF STANDARD

Installation - Provide planning, configuration and tentative schedule for the initial installation. This planning should involve collaborating with customer technical personnel to insure any and all critical elements and requirements regarding the environment are communicated. This process is envisioned as a collaborative effort between the vendor and customer with the end result being an installation that is 100 percent complete, functional and fully documented and the customer understanding everything needed to operate and maintain the system. This also includes demonstrating the steps necessary to backup and restore the system to a fully functional state. This entire process is to be conducted in such a manner as to minimize the impact to normal information systems operation.

Pre-configuration - To shorten the installation process and better utilize the time vendor personnel are on-site it is required pre-racking and pre-configuring the solution as much as possible prior to delivery. This includes working with customer personnel to develop any custom software images and preload the images prior to shipping.

Restorable images – In addition to having hardware preloaded with software a process must be in place to have restorable images for these systems as a backup to needing to overwrite/restore an existing image during install. Custom DVD's, portable storage, etc… are all viable options to having the image onsite for quick access and use.

Onsite impact – Minimal impact on the site facility is required. Efforts will be taken by the Vendor to ensure that the prep, assembly, install, and testing of the Solution will be done in a professional manner with minimal impact upon local site. Concern in regards to trash, path blockage, unsecured equipment, excessive levels of noise, etc… should be considered and action taken accordingly.

Necessary software/hardware – Aside from government-furnished property (GFP) referenced in the GFP section, all software and hardware required to make the Solution operational will be provided by the Vendor. This is to include but not limited to: cables, mounting brackets, screws, install software, testing equipment, etc…

Delivery – The Vendor will take responsibility of ensuring that all materials are delivered into the facility install location and the materials will remain the responsibility of the Vendor until acceptance testing is passed at all VA datacenters.

Trash – The Vendor will take responsibility of the removal of all trash from the facility, including but not limited to: boxes, packing materials, plastic bags, ties, etc…

OS installation and security – Following existing documentation provide by the VA Platform Server Team ensure all Operating systems and Security applications are installed accordingly.

EVALUATION FACTORS

- It is considered beneficial if the vendor can detail a delivery, installation and configuration plan for the equipment the vendor is proposing.
- Any demonstration that equipment can be pre-racked, pre-configured or pre-imaged is considered beneficial
- Verification that images can be restored onsite instead of remotely for install purposes is preferred.
- A basic plan to show minimal impact during installation and setup with certified technicians to follow this plan is preferred. Vendor hiring lowest cost "IT Talent" is not preferred.
- Checklists of hardware and software installation needs and verified availability of these is beneficial.

IMPLEMENTATION GUIDANCE

As much Vendor/VA staff preinstall communication to ensure full understanding is recommended.

Vendor verification of hardware fitting and requirements prior to install is required. Finding out at install that a piece of equipment does not fit or does not have all the install equipment is not acceptable.

All documentation, software, and hardware required for installation and operation of the Solution as well as training materials need to be onsite and verified for installation.

3.2.5 [TRAINING]

STANDARD

ID	Secondary Attribute	Specification
	Training Length	Provide equivalent of one hour of certified vendor classroom training for every TB of raw disk provided.
	Knowledge transfer	Work with VA staff as activities occur to ensure that VA can assume operational responsibility for the delivered solution.
	Documentation	Provide electronic copies of all materials, manuals, worksheets, etc. used in the delivery of the solution.

EXPLANATION OF STANDARD

Training Length – An initial complete training for VA staff is important for this project to succeed. An equivalent of one hour of certified vendor classroom training for every TB of raw disk provided, or more if the vendor believes this is needed.

VA support staff must have a level of trained knowledge provided to allow them to operate at a high level of expertise for day to day operations and standard problem resolution.

Knowledge transfer – While classroom training is important for the understanding of principles and procedures, actual knowledge transfer in regards to the implemented packages, how they work in the VA environment and potential improvement that may be available or upcoming is required.

Documentation – Initially all documentation for training, materials, worksheets, etc… for the initial installation must be provided in electronic format to ensure standard knowledge for all VA staff. As the product is changed and improved future training and documentation will also need to be provided.

Training documentation must be as complete as possible to allow for new VA staff to be able to understand and work with the vendor product.

EVALUATION FACTORS

- Vendor specific training that is oriented towards certification or “engineer” level training that is pertinent to properly managing and troubleshooting the product is preferred.
- Additional time/effort spent working with VA staff to ensure that the VA environment is optimized and meeting VA expectations is beneficial.
- When directly training VA staff printed as well as digital materials is beneficial to allow full potential of learning from staff.
- User forums for exchange of ideas and knowledge are preferred.

IMPLEMENTATION GUIDANCE

Any implementation that requires a strong base of knowledge for VA staff needs to have a planned training event set in place prior to installation to allow for full VA understanding and best potential for project implementation. While this training should be prior to installation it must not be so far in advance that newly learned skills/knowledge will become stale/obsolete by installation time.

In addition any installation that will occur near a time of a new patch or revision needs to ensure that the new knowledge is provided with the training.

3.3 [TIER 3 STORAGE SERVICE]

3.3.1 [STORAGE SUBSYSTEM HARDWARE (HW)]

STANDARD

ID	Secondary Attribute	Specification
	Workload	Capable to support Small and Low Performance Workload. Target performance would be retrieval of data file of 10 MB within 60 seconds of request.
	Minimum IO/sec	20,000 SPC-1 IOPS™ as measured by SPC-1 benchmark (http://www.storageperformance.org/results/))
	Minimum Throughput	1,000 or less SPC-2 MBPS™ as measured by SPC-2 benchmark (http://www.storageperformance.org/results/)
	Storage unit uptime	4'9s uptime.
	Universal Device ID value (UDID)	Not applicable.
	Redundancy	Fully redundant power supplies, cooling fans, component controllers, and others. All controllers within a single module will automatically fail over and load balance with one another. Controller module will support a minimum of two controllers.
	FC - Hosts to Storage Connectivity	Storage subsystems must support minimum four 4-Gbit/s Fiber Channel ports. Ability to support ports expansion to meet Tier 1 performance requirements in the same unit(s).
		Minimum two redundant multi-path connections from Host to Storage device. The Host connectivity throughput and performance will not be degraded even if 50% of the Host connectivity is lost.
	iSCSI - Hosts to Storage Connectivity	Storage subsystems must support minimum 1 Gb Ethernet connectivity with link aggregation. 10 Gb Ethernet support is preferred. Controller module will support a minimum of four Ethernet ports. Ability to support ports expansion in the same unit(s). Support Jumbo frame and LACP protocol.
		Minimum two redundant multi-path connections from Host to Storage device. The Host connectivity throughput and performance will not be degraded even if 50% of the Host connectivity is lost.
	SCSI Initiator (Host	Support a minimum of 256

	Connections)	
	Replication	Capable of synchronous and asynchronous replication with write order fidelity.
	LUN creation	Ability to create LUN across all spindles.
	LUN Expansion	Dynamic LUN expansion is required.
	Storage provisioning	Capable of over-provisioning or Over-allocation storage capacity that allows hosts to view more storage capacity than has been physically reserved on the storage array itself
	Tiering capability	Using policies to move inactive data to lower tier of storage
	Deduplication	Capable of supporting post process data deduplication.
	Snapshots	Capable of creating point in time delta snapshot Capable of creating space efficient snapshots on an as needed basis versus snapshot space reservation
	Clones	Capable of creating point in time delta clone Capable of creating space efficient clones on an as needed basis versus snapshot space reservation. Immediate access to clones before it is completed.
	Storage device scale up capability	Not applicable
	Supported Disk type	Ability to support sufficient disk drive technologies to meet Tier 3 performance requirements.
	Return disk option	Non-return disk option is required
	Interoperability - Industry standards	Each storage subsystem must provide Storage Management Initiative Specification (SMI-S) 1.1 conforming provider (http://www.snia.org/ctp/conformingproviders)
	Firmware and microcode upgrade or updates	Completely non-disruptive to operations firmware and microcode upgrade or updates for all components with zero downtime are required.
	Boot from SAN	Storage subsystem will support boot from San.
	Operating system and file system compatibility	Must support operating systems and their associated file systems as listed in the TRM.

	Applications compatibility (minimum)	Applications listed by VA Technical Reference Model (TRM) for enterprise deployment.
	Redundant Array of Independent Disk (RAID) levels	Minimum support for RAID 0+1/10/5/6 in same subsystems.
	RAID group size	Vendor offering must be able to meet storage capacity without exceeding 7 TB RAID group size and without exceeding 7 data drives.
	Power switches	Master power switches must be covered to prevent inadvertent activation.
	Standardized layouts	Components must be mounted in standardized configurations for all VA installations.
	Additional servers	Refer to Server Standard, Section Class C Server
	Role-based access	Solution must include security configurations that support role-based access required to limit functions during normal and COOP operation.
	Documentation	Provide detail design solution documents and drawings. All design methods and calculations to achieve the performance requirements must be clearly stated in the document. All assumptions if any must be included in the design document

EXPLANATION OF STANDARD

Workload – Capable of supporting low to medium performance workloads such as such as non-time sensitive operations and data archiving. Target performance would be retrieval of data file of 10 MB within 60 seconds of request.

Minimum IO/sec - The SPC-1 minimum benchmark as identified in this standard provides for a independent and objective measuring tool with regards to IOPS (Input/Output operations per second) for which all potential SAN Solutions can be gauged. Specific test include OLTP, database operations and mail server implementations. Specifically SPC-1 is defined by www.storageperformance.com as "a single workload designed to demonstrate the performance of a storage subsystem while performing the typical functions of business critical applications. Those applications are characterized by predominately random I/O operations and require both queries as well as update operations". **The specific benchmark value was determined based on analysis of major vendor SPC benchmark submissions.**

Minimum Throughput - The SPC-2 minimum benchmark as identified in this standard provides for an independent and objective measuring tool with regards to MBPS (megabits per second) transfer rates for which all potential SAN Solutions can be gauged. Specific tests include large file processing, large database queries and video on demand (VOD). Specifically SPC-2 is defined by www.storageperformance.com as "three distinct workloads designed to demonstrate the performance of a storage subsystem during the execution of business

critical applications that require the large-scale, sequential movement of data. Those applications are characterized predominately by large I/Os organized into one or more concurrent sequential patterns. A description of each of the three SPC-2 workloads is listed below as well as examples of applications characterized by each workload". **The specific benchmark value was determined based on analysis of major vendor SPC benchmark submissions.**

Storage unit uptime- In normal operation, the subsystem should not require more than fifty two minutes interruption in a year for software upgrade or component replacement. Uptime is all connected hosts able to continue processing data. Additional Information can be gathered at http://www.uptimeinstitute.org.

Redundancy – Failure of a single component will not stop storage system operation in any capacity. Fully redundant storage systems are critical to the continuing processing and to maintain system stability.

FC – Host to Storage Connectivity – Storage subsystem must have multiple 4 Gb/second connectivity. An 8/GB connection is highly desirable.

iSCSI – Hosts to Storage Connectivity - For interoperability the SAN Solution that is procured must provide current iSCSI capabilities of 1GB current connectivity and the ability to upgrade to future higher speed connectivity. Additionally, Link Aggregation with dual NICS support is required.

SCSI Initiators (host connections) – a SCSI initiator is the host-side endpoint of a SCSI session. Every redundant host connection requires two SCSI initiators.

Replication – Replication is typically a software function, but hardware must support replication

LUN creation – The ability to create LUN's 'on the fly' without outage to the system and without disruption to the host systems.

LUN Expansion – Ability to add space to a LUN without rewriting data on that LUN.

Storage provisioning – Commonly called "thin provisioning". Thin provisioning is typically a software function, but hardware must support it.

Tiering capability - Manually or automatic policies to move inactive data to lower tier of storage, either in same or other frame. Tiering is typically a software function, but hardware must support it.

Deduplication – Data Deduplication is a technology strives to reduce the amount of duplicate data being backed up and then stored. The technologies identify and eliminate common data in and across backup streams. By eliminating the common objects, the resulting storage requirement will be reduced.

Global deduplication comes into play when you have multiple deduplication devices. With multiple deduplication devices nodes, when data that is seen before by one node is sent to a second node, the second node knows that data has already been stored and it will not be stored for a second time.

Snapshots – Snapshots are typically a software function, but hardware must support data snapshots (copy on write)

Clones – LUN cloning is typically a software function, but hardware must support data clone (full copies)

Supported Disk type - As a minimum the SAN solution will provide the ability to utilize and support Fibre Channel drives, SATA drives and any near horizon drive technology (i.e. Solid State Drives) within the same SAN system.

Return disk option - As part of the support contract any failed disk within the SAN device or accompanying management servers will not be returned to the vendor. They will be maintained, secured and destroyed in accordance with applicable VA regulations with regards to data destruction.

Interoperability - Industry standards - for consistency and to ensure that the SAN Solution provided meets the criteria set forth by both Industry Standards and the VA Standard a baseline of specifications are needed. These specifications are best indicated by the Storage Management Initiative Specification (SMI-S) which was developed by leading storage equipment and software providers.

Firmware and microcode upgrade or updates - The capabilities to perform firmware and microcode updates without interrupt to the operations of the SAN and hosts devices connected there to. This is to include, but not limited to, disk firmware, controller firmware, controller software, and internal SAN Fabric switches.

SAN boot support (minimum) - The ability to provide the operating system of a host server to boot directly from the SAN device without local server disks is required. Please see the Operating Systems as listed in VA Technical Reference Model.

Operating system compatibility (minimum) - Please see the Operating Systems as listed in VA Technical Reference Model (TRM). The current VA TRM will be provided by COTR during acquisition process

Applications compatibility (minimum) - Please see the Applications as listed in VA Technical Reference Model. The current VA TRM will be provided by COTR during acquisition process.

Redundant Array of Independent Disk (RAID) levels - Due to the varying needs and uses the SAN Solution will be required to support the capabilities of RAID1, RAID5 and RAID6 in the same storage subsystems and disk enclosure. While above is a minimum RAID levels additional RAID configuration support is desired.

RAID group size - The size limit for a RAID group must not exceed 7TB in order to obtain optimal performance. The size requirement for a RAID group is based on the ability to rebuild the RAID group following a disk failure. Based on a drive MTTF of 1,000,000 hours, a RAID-5 group larger than 7 TB has a high risk of not being able to successfully rebuild without an unrecoverable error (URE). The existence of 7 drives to a RAID set is optimal and is the recommend amount to be allocated to any given RAID drive set.

Power switches - In addition to being redundant all power switches and power plugs must be properly secured and encased to ensure that they cannot be accidentally tripped, unseated or create any situation where power will be disrupted to the devices they are providing power to.

Standardized layouts - The layout of the solution must be a consistent design that is in use at all datacenters that are keeping with VA standards. This approach allows for the redistribution of the equipment to different sites and the most efficient use of data center space.

Additional servers - SAN support is often managed via a dedicated server(s). These hosts must be supported by the same support contract and remote management. Additionally all host must adhere to all the VA security policies and procedures with relation to servers, must be FIPS140-2 compliant and have only VA approved software installed.

Role-based Access - The ability for the applicable support personnel to manage the SAN solution and support servers from an industry standard out of band management solution is required and critical. Due to the remote nature and decentralized nature of support personnel must be able to access the SAN and servers even while shutdown or during BIOS/POST operations.

Documentation - Documentation must be provided that is described in the standard that allows for the complete understanding of the solution that is implemented. The importance of this is to create a seamless handoff from the varying organizations that will be supporting the SAN solution

EVALUATION FACTORS

Lowest Total Cost of Ownership (TCO) solution that meets the performance requirements is preferred. Components considered are small footprint, power consumption, cooling, Hardware, Software, license, Overhead cost of managing the devices, Ease of Management, Acquisition cost, Maintenance and deployment costs, storage capacity (such as number of data copies),Information Lifecycle Management(ILM) cost.

Workload – The use of industry standard tools and benchmarks to provide adequate levels of validation during the acquisition process is critical to ensure the system procured can handle the rigors and high demands set forth in this tier.

Minimum IO/sec - The threshold of 20,000 IOPS using this SPC-1 benchmark has been identified as the minimum to provide the needs of the VistA application.

Minimum Throughput -The threshold of 1,000MBPS using this SPC-2 benchmark has been identified as the minimum to provide the needs of the VistA application.

Storage unit uptime – REQUIRED as defined in the standard above for this Tier. This would be 4 nines which equates to 52.6 minutes per year.

Redundancy – REQUIRED Redundant components are needed to ensure the failure of one component of the storage system will not cause an outage.

FC – Hosts to Storage Connectivity – REQUIRED 4/GB connections however 8/GB connections are highly desirable and requested.

iSCSI – Hosts to Storage Connectivity – REQUIRED with minimum current iSCSI capabilities of 1GB connectivity with 10GB preferred and or expandable to in future.

SCSI Initiators (host connections) – a SCSI initiator is the host-side endpoint of a SCSI session. Every redundant host connection requires two SCSI initiators. The greater the available space to be assigned (usable) the more initiators would be required. Suggest at least one SCSI initiator for every two drive slots or 256 minimum.

Replication – Storage subsystem must support asynchronous and synchronous HA and DR replication

LUN Creation – LUN creation is a must in the type of environment that this tiered solution will be placed.

LUN Expansion – REQUIRED

Storage provisioning – Function included in cost. Thin provisioning is typically a software function, but hardware must support it.

Tiering capability – Function included in cost. Thin provisioning is typically a software function, but hardware must support it. Array needs to support or include multiple drive types or if tiering will be between multiple storage subsystems of heterogeneous types.

Deduplication – Source, target, inline, or post process deduplication. The deduplication method used must not degrade overall application performance, storage performance, and will not reduce backup windows. Support Global deduplication is preferred.

Capable of perform both file-level, and block-level data deduplication is preferred.

Capable of perform both file-level and block-level data deduplication on primary storage is preferred.

Snapshots – Compare limits on number of snapshots that can be made of a primary storage LUN

Clones – Compare limits on number of snapshots that can be made of a primary storage LUN

Storage device scale up capability – REQUIRED Evaluate based on expandability of usable storage in TB

Supported Disk type - REQUIRED the supported disk type must be specified in all documentation as to the exact type, speed and capacity.

Return disk option - REQUIRED To be documented in the procurement that no failed disks will be returned to vendor or leave in the possession of the VA at all times until properly disposed.

Interoperability – Industry standards – REQUIRED the supporting documentation should be presented and validated during the acquisition process. These specifications are SMI-S v1.1 as described at: http://www.snia.org/forums/smi/tech_programs/smis_home/

Firmware and microcode upgrade or updates – REQUIRED the means at which the vendor's solution will accomplish this task needs to be documented and tested prior to acceptance of the solutions.

SAN boot support (minimum) - REQUIRED to support the operating systems listed are required within this document

Operating system compatibility (minimum) – At a minimum the supported solution will provide OS support for Windows based Operating System, Linux Based Operating System, UNIX based Operating System and OpenVMS Operating System. The current VA TRM will be provided by COTR during acquisition process.

Applications compatibility (minimum) – The current VA TRM will be provided by COTR during acquisition process.

Redundant Array of Independent Disk (RAID) levels should meet the current and future needs of the VA. While the current VistA "Production data" resides on mirrored RAID1 drives the ability to augment them with addition RAID types is important. Raid group sizing limitations of Terabytes and number of physical drives is needed and should be evaluated as part of the acquisition process.

RAID group size - The size limit for a RAID group must not exceed 7TB in order to obtain optimal performance. The total number of drives assigned to a particular RAID set must not exceed seven physical drives. This is to ensure the integrity of the RAID group.

Power switches - All power switches and power plugs must be properly secured and encased

Standardized layouts - Layout and plan design will need to be validated during the acquisition process

Additional servers - All additional servers should be identified during the procurement process and keep with the VA Server Standards.

Role-based Access - Refer to Server Standard, Section Class C Server

Documentation - Cost of documentation should be identified and included in the procurement process. Vendor shall provide electronic, three dimensional models of equipment proposed for use with CAD and visual design/planning applications.

IMPLEMENTATION GUIDANCE

Lowest Total Cost of Ownership (TCO) solution that meets the performance requirements is preferred.

Workload- The use of industry standard tools and benchmarks to provide adequate verifications levels during acceptance testing

Minimum IO/sec – Include validation in acceptance testing

Minimum Throughput – Include validation in acceptance testing

Storage Unit Uptime – Include validation in acceptance testing

Redundancy – Include validation in acceptance testing**.** Component failure testing should occur prior to putting into production. This should include a planned failure of a single component to ensure the backup/ secondary component provides adequate coverage to verify no outage of the storage system.

FC - Hosts to Storage Connectivity – Recommend 8/GB Fibre Channel connections to host.

iSCSI - Hosts to Storage Connectivity – Include validation in acceptance testing

iSCSI Initiator (Host Connections) - Include validation in acceptance testing

Replication – Testing of the replication process should occur during acceptance testing.

LUN Creation - Testing and actual creation for production should occur during acceptance testing to provide validation.

LUN Expansion – Include validation in acceptance testing

Storage Provisioning – Include validation in acceptance testing

Tiering Capability – If software is in place and capabilities exist the testing of this function should be conducted from this tier to a lower (or higher) tier.

Deduplication – Must test and validate to ensure the deduplication method used does not degrade overall application performance, storage performance, and will not reduce backup windows. Test and validate to ensure Global deduplication only process on copy of data among sites.

Snapshots – Include validation in acceptance testing

Clones – Include validation in acceptance testing

Supported Disk type - Fiber Channel and iSCSI are needed at a minimum.

Return disk option - Not applicable other than being aware of if any disk failure during implementation.

Interoperability – Industry standards - The standards which are provided in the sections above must be adhered to and validated during the implementation phase using the common set of tools identified in the SMI-S v1.1.

Firmware and microcode upgrade or updates - The means this is achieved by the SAN Solution needs to be tested.

SAN boot support (minimum) – Test and implement during installation with validation in acceptance testing

Operating system compatibility (minimum) - Include validation in acceptance testing

Applications compatibility (minimum) - Include validation in acceptance testing

Redundant Array of Independent Disk (RAID) levels - Include validation in acceptance testing

RAID group size - Include validation in acceptance testing

Power switches - All power switches and power plugs must be properly secured and encased. This also includes the proper covering of any emergency cutoff switches.

Standardized layouts - Ensure that all layouts conform to VA Standard and are validated during installation.

Additional servers - Operating System and Applications must be VA Server Standard. The current VA TRM will be provided by COTR during acquisition process. Refer to Server Standard, Section Class C Server

Role-Based Access – Described and documented in the support contract.

Documentation - All documentation should be in the form in a standard form that can be used by all VA support staff (i.e. Word documents, pdf or Visio).

3.3.2 [STORAGE MANAGEMENT SOFTWARE]

STANDARD

ID	Secondary Attribute	Specification
	Enterprise license not based on capacity	Software licenses provided must be perpetual with a five-year support and update subscription, with all licenses and rights transferred to the Government at the time the installation is completed. Licenses must be transferable without limitation and provisioned as a VA enterprise license, without additional storage allocation-based charges, such as per GB or TB.
	Interoperability	Management software must be listed as a Storage Networking Industry Association (SNIA) SMI-S 1.1 conforming client. (http://www.snia.org/forums/smi/tech_programs/ctp/smi_conform/smi_client/smi_client_definitions.
	Storage Reporting	Storage reporting components suitable for use in a fee for service, chargeback environment. Automated reports of storage allocations must be capable of being generated by non-IT staff. Must support ODBC and/or JDBC connectivity.
	Automated tools for LUN provisioning	The software should have automated tools to provision a large number of Disk Groups and LUNs. Similarly, an automated solution should be provided to configure hosts with large numbers of logical disks.
	Proactive monitoring and remote notification	The management tool must be capable of proactive monitoring and remote notification of system and application health. Must support ODBC and/or JDBC connectivity.
	Single storage management console	Storage hardware must be manageable from a single storage management application and with the capability of automatic discovery of equipment connected to the SAN.
	Additional servers	Refer to Server Standard, Section Class C Server
	Management server security	Refer to Server Standard, Section Class C Server
	Data snapshot (local)	License and annual maintenance (5 years) as required for software to support array-based point-in-time data images suitable for use for administrative tasks such as online backup & testing with no impact to source data and minimal additional space requirements.

	Performance analysis	Performance management software to monitor, analyze and report on all solution components (i.e. from host to fabric to storage). This includes storage subsystems, software operations, SAN infrastructure, replication and telecommunications. Software should be able to identify and analyze response time, and other relevant metrics to enable identification and resolution of potential bottlenecks. The tool must support OpenVMS client operating system. All management software must be ODBC and/or JDBC connectivity.
	Storage Capacity planning	The software must be able to analyze current capacity and forecasts future system requirements. The software should be able to collect component data to project future usage of the storage system.
	Local copy	License and annual maintenance (5 years) as required for software to support local array-array LUN copy/replication.
	Consistent design	All software should use identical components where possible to facilitate common updates across the solution.

EXPLANATION OF STANDARD

Enterprise license not based on capacity – to include 5 years of support as required for enterprise SAN Management application. Licenses must be transferable without limitation and provisioned as a VA enterprise license, without additional storage allocation-based charges, such as per GB or TB.

Interoperability - Management software must be listed as a Storage Networking Industry Association (SNIA) SMI-S 1.1 conforming client.
(http://www.snia.org/forums/smi/tech_programs/ctp/smi_conform/smi_client/smi_client_definitions

Storage Reporting – Access level reporting with the ability to generate reports by non-IT staff.

Automated tools for LUN provisioning - a single, intelligent interface that allows you to provision storage systems and fabric switches from end-to-end. The software should have automated tools to provision a large number of Disk Groups and LUNs along with the ability to configure hosts with large numbers of logical disks.

Proactive monitoring and remote notification - Storage Management software must be capable of monitoring and remote notification in the event of an alert, failure or the inability of the system to meet the customer's SLA's. Provisioning actions to trigger events, SNMP traps, and policies for notification. Ability to send email or custom scripts or programs for notification.

Single Storage Management console – Storage hardware must be manageable from a single storage management application.

Data snapshot (local) - License and annual maintenance (5 years) as required for software to support array-based point-in-time data images suitable for use for administrative tasks such as online backup & testing with no impact to source data and minimal additional space requirements.

Performance analysis – Storage management software to monitor, analyze and report on all solution components (i.e. from host to fabric to storage). This includes storage subsystems, software operations, SAN infrastructure, replication and telecommunications. Software should be able to identify and analyze response time, and other relevant metrics to enable identification and resolution of potential bottlenecks.

Storage Capacity planning - The software must be able to analyze current capacity and forecasts future system requirements. The software should be able to collect component data to project future usage of the storage system.

Local copy - License and annual maintenance (5 years) as required for software to support local array-array LUN copy/replication.

Consistent Design – All software should use identical components where possible to facilitate common updates across the solution.

EVALUATION FACTORS

- Enterprise Level Storage Management software
- Ability to manage multiple devices
- Enterprise License w/5years annual maintenance
- Storage Management Reporting
- Performance Monitoring
- Single Storage management console
- Ability to Manage events and policies

IMPLEMENTATION GUIDANCE

Implementation should include all optional software needed to meet the requirements listed above. Licensing and maintenance terms should the Hardware/Software Technical Support sections of this document. Professional implementation services should be included along with “classroom” training for support staff as outlined in the Training sections of this document.

3.3.3 [HARDWARE/SOFTWARE TECHNICAL SUPPORT]

STANDARD

ID	Secondary Attribute	Specification
	Support procedures	Documented support/escalation procedure for all components of the solution.
	Support Availability	Software support required 24x7x365 for all software provided in the solution. License and annual maintenance 3 years with 2 extension years.
		Hardware Maintenance/Support 5 yr, 24x7x365, 4 hour response time is required.
	License transfer	Licenses can be transferred without limitation within the Department of Veterans Affairs.
	OEM resources	Direct access to on-line OEM vendor support incident information and tracking.
	Support Interface	All VA datacenters must have access to incident information and tracking for all VA datacenters.
	Disruptive patches	Describe any type of updates/patch that would require a hosted service outage of the solution.
	SLAs	Documented Service Level Agreements (SLAs) for support requests.
	Professional services	Include cost of any professional services for services that must be completed by the vendor.

EXPLANATION OF STANDARD

Support procedures – A documented (digital & printed) set of instructions and escalation procedures to include updated contact information for the appropriate point of contact while troubleshooting problems. This will be a living document and as such digital copies should have supplements/replacements provided quarterly to ensure the most up to date procedures are available for the customer.

A concisely documented set of procedures is essential for communication between the customer and the support staff, allowing for all parties to know when priority escalation occurs, how it occurs, and the proper path for the expedited resolution.

Support Availability – Due to the criticality of these systems, full round the clock support is essential for a minimum of the first year, with options available to extend for the following four years allowing for a total of five years. In addition a minimal 4 hour response time in regards to hardware maintenance is required.

License transfer – All pertinent licenses must be capable of being transferred between various VA sites and cannot be restricted by location. Due to the nature of the OI&T structure for the VA licenses must be capable of being transferred within the various physical locations without restriction.

OEM resources – Direct communication paths to the knowledge experts of a product is key for fast response and ensuring the systems remain operational at the levels needed. Being required to go through middlemen in efforts to funnel trouble calls is not suitable to the nature of these systems.

Speaking directly with the product expert allows for potential miscommunication errors to be avoided. Being able to go directly to the appropriate level of tier knowledge on a failure is essential for ensuring that the problem is communicated correctly and quickly the best support engineer that can assist the customer.

Support interface – Due to many VA experts working across various regions and areas it is vital for all site's to be able to access VA wide information for troubleshooting and sharing of information.

VA I.T. support is organized through a central Office of Information Technology and is required to assist each various region/area as needed. Support contact and information should not be limited to a locality and must allow for access across the VA areas.

Disruptive patches – Ideally updates/patches will be able to be implemented with 0% system downtime. Any operations that would require a system outage needs to be documented and provided for review.

VA standards require that all disruptions be documented, submitted, and tracked to resolution. Known procedures that require disruption of service need to be documented and said documentation made available. Support engineers will need to work with VA staff to ensure that the required procedures for disruptions are followed.

SLAs - Documented Service Line Agreements (SLAs) for support request will be provided and the Vendor will ensure that there is no confusion between VA staff and Vendor on expectations.

Professional services – Provide a full disclosure of vendor specific services that must be provided by the vendor only. I.E. Some storage systems require a vendor engineer to flash firmware or similar upgrades and do not allow the customer to perform such actions.

VA standards require that outside contractors be escorted and/or evaluated for security requirements. All expected procedures that require vendor services need to be provided and a list of potential engineers that will be onsite updated as needed to ensure the engineer can gain access.

EVALUATION FACTORS

- Quality of documentation to include ease of finding information, extent of informative data, and usability in regards to trouble shooting and technical support will be considered.

- Direct phone contact for immediate escalation of troubleshooting over email, web interface, or other "automated" trouble shooting requests will be preferred.
- While direct access to product experts are needed, having a support engineer/contact to supervise and ensure that all experts are moving forward with the end goal of problem expedient problem resolution is preferred.
- Central/Single Interface for multiple sites to track VA related problems will be preferred.
- Minimum amount of scheduled downtime for patching/updating and supporting evidence for such is preferred.
- Path of communication for VA to suggest improvements and see improvements implemented is beneficial.
- Forums or other user group discussion areas are beneficial.
- Lower on-site response time is beneficial.
- Lower initial "engineer level" contact response time is beneficial.
- Lower time-to-repair is beneficial.
- Vendor-supplied components stocked as spares near, or at, facility is beneficial.
- Penalty clauses for vendor not meeting support contract provides is beneficial.

IMPLEMENTATION GUIDANCE

Coordination with initial VA staff for knowledge transfer and verified understanding is important. Continuing contact with VA staff to ensure support procedures are viable and procedures in place for VA input to improve support/product is essential.

3.3.4 [HARDWARE/SOFTWARE INSTALLATION]

STANDARD

ID	Secondary Attribute	Specification
	Installation	Provide hardware/software installation, including initial configuration, Storage Area Network configuration & knowledge transfer.
	Pre-configuration	Rack mount and configure the solution (including servers and storage where possible) prior to shipping it to the VA. This minimizes the on-site installation time as well as the number of crates and boxes that must be received and tracked by VA.
	Onsite impact	All on-site activities must be conducted in such a manner as to minimize the impact to normal information systems operations.
	Necessary software/hardware	Provide all necessary hardware and software, including all necessary cables and mounting hardware to make the Solution operational, except government-furnished property (GFP) referenced in GFP section.
	Delivery	Provide inside delivery, installation and insurance of all equipment to VA datacenters. The VA does not accept delivery of the equipment until acceptance testing is passed at all VA datacenters.
	Trash	Remove all trash associated with shipping, delivery and installation.
	OS installation and security	Refer to Server Standard, Section Class C Server

EXPLANATION OF STANDARD

Installation - Provide planning, configuration and tentative schedule for the initial installation. This planning should involve collaborating with customer technical personnel to insure any and all critical elements and requirements regarding the environment are communicated. This process is envisioned as a collaborative effort between the vendor and customer with the end result being an installation that is 100 percent complete, functional and fully documented and the customer understanding everything needed to operate and maintain the system. This also includes demonstrating the steps necessary to backup and restore the system to a fully functional state. This entire process is to be conducted in such a manner as to minimize the impact to normal information systems operation.

Pre-configuration - To shorten the installation process and better utilize the time vendor personnel are on-site it is required pre-racking and pre-configuring the solution as much as possible prior to delivery. This includes working with customer personnel to develop any custom software images and preload the images prior to shipping.

Restorable images – In addition to having hardware preloaded with software a process must be in place to have restorable images for these systems as a backup to needing to overwrite/restore an existing image during install. Custom DVD's, portable storage, etc… are all viable options to having the image onsite for quick access and use.

Onsite impact – Minimal impact on the site facility is required. Efforts will be taken by the Vendor to ensure that the prep, assembly, install, and testing of the Solution will be done in a professional manner with minimal impact upon local site. Concern in regards to trash, path blockage, unsecured equipment, excessive levels of noise, etc… should be considered and action taken accordingly.

Necessary software/hardware – Aside from government-furnished property (GFP) referenced in the GFP section, all software and hardware required to make the Solution operational will be provided by the Vendor. This is to include but not limited to: cables, mounting brackets, screws, install software, testing equipment, etc…

Delivery – The Vendor will take responsibility of ensuring that all materials are delivered into the facility install location and the materials will remain the responsibility of the Vendor until acceptance testing is passed at all VA datacenters.

Trash – The Vendor will take responsibility of the removal of all trash from the facility, including but not limited to: boxes, packing materials, plastic bags, ties, etc…

OS installation and security – Following existing documentation provide by the VA Platform Server Team ensure all Operating systems and Security applications are installed accordingly.

EVALUATION FACTORS

- It is considered beneficial if the vendor can detail a delivery, installation and configuration plan for the equipment the vendor is proposing.
- Any demonstration that equipment can be pre-racked, pre-configured or pre-imaged is considered beneficial
- Verification that images can be restored onsite instead of remotely for install purposes is preferred.
- A basic plan to show minimal impact during installation and setup with a certified technicians to follow this plan is preferred. Vendor hiring lowest cost "IT Talent" is not preferred.
- Checklists of hardware and software installation needs and verified availability of these is beneficial.

IMPLEMENTATION GUIDANCE

As much Vendor/VA staff preinstall communication to ensure full understanding is recommended.

Vendor verification of hardware fitting and requirements prior to install is required. Finding out at install that a piece of equipment does not fit or does not have all the install equipment is not acceptable.

All documentation, software, and hardware required for installation and operation of the Solution as well as training materials need to be onsite and verified for installation.

3.3.5 [TRAINING]

STANDARD

ID	Secondary Attribute	Specification
	Training Length	Provide equivalent of one hour of certified vendor classroom training for every TB of raw disk provided.
	Knowledge transfer	Work with VA staff as activities occur to ensure that VA can assume operational responsibility for the delivered solution.
	Documentation	Provide electronic copies of all materials, manuals, worksheets, etc. used in the delivery of the solution.

EXPLANATION OF STANDARD

Training Length – An initial complete training for VA staff is important for this project to succeed. An equivalent of one hour of certified vendor classroom training for every TB of raw disk provided, or more if the vendor believes this is needed.

VA support staff must have a level of trained knowledge provided to allow them to operate at a high level of expertise for day to day operations and standard problem resolution.

Knowledge transfer – While classroom training is important for the understanding of principles and procedures, actual knowledge transfer in regards to the implemented packages, how they work in the VA environment and potential improvement that may be available or upcoming is required.

Documentation – Initially all documentation for training, materials, worksheets, etc… for the initial installation must be provided in electronic format to ensure standard knowledge for all VA staff. As the product is changed and improved future training and documentation will also need to be provided.

Training documentation must be as complete as possible to allow for new VA staff to be able to understand and work with the vendor product.

EVALUATION FACTORS

- Vendor specific training that is oriented towards certification or “engineer” level training that is pertinent to properly managing and troubleshooting the product is preferred.
- Additional time/effort spent working with VA staff to ensure that the VA environment is optimized and meeting VA expectations is beneficial.
- When directly training VA staff printed as well as digital materials is beneficial to allow full potential of learning from staff.
- User forums for exchange of ideas and knowledge are preferred.

IMPLEMENTATION GUIDANCE

Any implementation that requires a strong base of knowledge for VA staff needs to have a planned training event set in place prior to installation to allow for full VA understanding and best potential for project implementation. While this training should be prior to installation it must not be so far in advance that newly learned skills/knowledge will become stale/obsolete by installation time.

In addition any installation that will occur near a time of a new patch or revision needs to ensure that the new knowledge is provided with the training.

3.4 [GENERAL STORAGE AREA NETWORK (SAN)]

3.4.1 [LAN CONNECTIVITY]

STANDARD

ID	*Secondary Attribute*	*Specification*
	IP Connectivity between Hosts and Storage device	Minimum 1 Gb Ethernet and 10 Gb Ethernet is preferred. Support Jumbo frame and LACP protocol.
		Support multi-pathing from Hosts and Storage devices.
		Storage Data connection should be logically separate from production LAN data connection.
		Primary storage data connection should be logically separate from replication data connection.

EXPLANATION OF STANDARD

IP Connectivity between Hosts and Storage device - Minimum 1 GB Ethernet and 10 GB Ethernet is preferred. Support Jumbo frame and (LACP) Link Aggregation Control Protocol. Link aggregation or IEEE802.1AX-2008 is a computer networking term which describes using multiple network cables/ports in parallel to increase the link speed beyond the limits of any one single cable or port, and to increase the redundancy for higher availability.

Local SAN fabric must be isolated from replication SAN fabric thru logical and physical zoning with intelligent network services which would support logically isolated path groupings.

EVALUATION FACTORS

-

IMPLEMENTATION GUIDANCE

3.4.2 [FABRIC SWITCH HARDWARE (HW)]

STANDARD

ID	Secondary Attribute	Specification
	Fabric Connectivity between Hosts and Storage device	Redundant Switch Control (Supervisor) Card
		Fiber Channel Protocol
		Minimum 4-Gbit/s Fiber Channel Ports
		All fiber Channel switch ports will be autosensing to 1, 2, 4 or 8Gb
	Interoperability	Compatible with equipment from Cisco, Brocade and Nortel hardware.
	Fabric Isolation	Local SAN fabric must be isolated from replication SAN fabric
	Capacity "Throughput"	Isolate data and devices within a fabric, and configurable throughput for specific applications. Supports at least 1 Tbps of internal bandwidth in a single chassis (switch enclosure).
	Capacity "Ports"	384 FC ports in a single chassis (switch enclosure). Able to provision additional SAN ports without interruption.
	Port virtualization	Support N Port Virtualization.
	Manageability	Manageable from a single application.
	Fully redundant configuration	Provide fully redundant configuration
	Oversubscription	Provide no more than 4:1 over subscription at 4 Gbps.
	Fabric	SAN switch shall support redundant fabrics.
	Automated monitoring	SAN switches must implement automated monitoring and phone-home support configurations over IP.
	Current generation equipment	Fiber channel switches and/or components must not be listed on vendor websites as "end of life" or "end of sale" or "end of service life". The initial hardware general availability date should be less than 5 years from the proposal submission date.
	Additional ports	Solution must provision additional SAN ports required to fully connect

		solution components (storage subsystems, inter-switch links, management hosts, replication hardware, etc) in addition to host requirements.
	Rack Configuration	Provide appropriate 4 posts (42 or 47 U) with sidewalls.
	Manageable power supplies	Redundant IP Manageable & Accessible Power Distribution Unit (PDUs) sufficient to power all units in the rack.
	Cooling	Fans (N+1) on switch and cabinet to support airflow requirements.
	Physical layout	All components must be easily accessible without having to de-install, disconnect or remove other components so that service can be easily accomplished.
	Standardized layouts	Components must be mounted in standardized configurations for all VA installations.
	Additional servers	Refer to Server Standard, Section Class C Server
	Role-based access	Solution must include security configurations that support role-based access required to limit functions during normal and COOP operation.

EXPLANATION OF STANDARD

Fabric Connectivity between Hosts and Storage device-Fiber Channel protocol widely used throughout the VA. Minimum of 4 GB Fiber Channel port speed, this is a mature & widely used technology. It is less expensive due to wide availability of this technology. This proven technology is stable and efficient throughout the Enterprise market. Supervisor Cards able to operate in either Active/Active or Active/Passive Mode. Ability to upgrade or replace any component without interruption during normal operation. Fiber Channel LC connector required.

Interoperability - Architecture of the Fabric switch should enable multilayer and multiprotocol functionality.

Fabric Isolation – Local SAN fabric must be isolated from replication SAN fabric (FCIP) thru logical and physical zoning with intelligent network services which would support logically isolated path groupings.

Capacity "Throughput" – Best Practice with "single initiator zones" is to create zones based on the initiator; each zone will contain a single Host, or initiator. Multiple storage array ports can be added to the zone without violating the single initiator rule-arrays are targets.

Capacity "Ports" – Switch enclosure to allow min. of 10 slots for port cards. Able to provision additional SAN ports without interruption Switch should support hardware based integrated port-level routing.

Port virtualization - Support N Port Virtualization with NPV or similar technology

Manageability - Manageable from a single application which can access to all components in the SAN fabric switches.

Fully redundant configuration – Ability of switch firmware or hardware to retain a copy of the current configuration and the previous configuration.

Oversubscription - allow over subscription depending on port activity.

Fabric – SAN Fabric switch, appropriate in a data center environment must be flexible and saleable. Ability to upgrade or replace any component without interruption during normal operation.

Automated Monitoring – SAN switches must implement automated monitoring and phone-home support configurations over IP. The ability to notify via multiple methods (example: email) any selected alerts that occur within the SAN fabric switches.

Current Generation Equipment - Fiber channel switches and/or components must not be listed on vendor websites as "End of Life" , "End of Sale" or "End of Service Life". The initial hardware general availability date should be less than 5 years from the proposal submission date.

Additional ports - Solution must be able to provision additional SAN ports without interruption. Support a verity of port types and capable of advanced traffic management.

Rack Configuration - Provide appropriate 4 posts (42 or 47 U) with sidewalls as specified by VA requirements.

Manageable Power Supplies – Ability to manage thru an API or other standard interface from a remote location all power metrics of the PDU's.

Cooling – Switch enclosure able to lose one fan without any impact to enclosure (N+1).

Physical Layout – All components must be easily accessible without having to de-install, disconnect or remove other components so that service can be easily accomplished. This requires that all components within the SAN fabric switches be able to be replaced or upgraded without removing another component, this includes not blocking or restricting access to another component via cables or brackets.

Standardized layouts - The layout of the solution must be a consistent design that is in use at all datacenters that are keeping with VA standards. This approach allows for the redistribution of the equipment to different sites and the most efficient use of data center space.

Additional Servers – Refer to Server Standards, Section Class C Server

Role-Based Access - Solution must include security configurations that support role-based access required to limit functions during normal and COOP operation. This role-based access should be granular and meet all VA security requirements.

EVALUATION FACTORS

- Lowest Total Cost of Ownership (TCO) solution that meets the performance requirements is preferred. Components considered are small footprint, power consumption, cooling, Hardware, Software, license, Overhead cost of managing the devices, Ease of Management, Acquisition cost, Maintenance and deployment costs.
- Support for FCoE protocol is highly desirable.
- Support for iSCSI protocol is highly desirable.

- Support for FICON connectivity is highly desirable.

IMPLEMENTATION GUIDANCE

Lowest Total Cost of Ownership (TCO) solution that meets the performance requirements is preferred.

Fabric and Topology, Vista requires up to 10 logically isolated path groups in a SAN fabric to be shared between its two metro data centers, this allows this application the ability to meet its redundancy and availability requirements.

Synchronous replication over FCIP between Metro Data centers for HA, which is widely used in VA Vista application.

Oversubscription - no more than 4:1 over subscription with 4 GBs ports in a SAN fabric used with the Vista application.

3.4.3 [SAN MANAGEMENT SOFTWARE]

STANDARD

ID	***Secondary Attribute***	***Specification***
	Management Software	Enterprise level SAN management software Automatic configuration checking for SAN configuration, updates and reconfigurations. Automatic discover of equipment connected to the SAN Manage multiple devices in a selected domain. Wizards for common tasks such as zone configuration, , Fiber Channel over IP (FCIP) tunnels, and access control lists (ACLs) Fabric Interoperability – work with SAN switches regardless of vendor Must support ODBD and JDBC connectivity
	Interoperability	Management software must be listed as a Storage Networking Industry Association (SNIA) SMI-S 1.1 conforming client. (http://www.snia.org/forums/smi/tech_programs/ctp/smi_conform/smi_client/smi_client_definitions.
	SAN Reporting	SAN reporting components suitable for use in an enterprise environment. Automated reports of storage allocations must be capable of being generated by non-IT staff. Must support ODBC and/or JDBC connectivity.
	Proactive monitoring and remote notification	The management tool must be capable of proactive monitoring and remote notification of system and application health. Must support ODBC and/or JDBC connectivity.
	Performance monitoring	Performance statistics for Inter-Switch Links (ISLs), host and storage device connections, and traffic between specific Fiber Channel sources and destinations (flows) Ability to set performance threshold based on manual entry or calculated based on previous measurements. Historical performance reports and graphs over daily, weekly, monthly, and yearly intervals; Top 10 and daily summary reports for all ISLs, hosts, storage connections, and flows.

		Performance reports should be accessible without privileged access to the SAN switch.
	Single SAN management console	SAN hardware must be manageable from a single storage management application and with the capability of automatic discovery of equipment connected to the SAN.
	Additional servers	Refer to Server Standard, Section Class C Server
	Management server security	Refer to Server Standard, Section Class C Server
	Consistent design	All software should use identical components where possible to facilitate common updates across the solution.

EXPLANATION OF STANDARD

Management Software – Must have Enterprise level management for heterogeneous, physical and virtual host Infrastructure. Automatic configuration checking for SAN configuration, updates and reconfigurations. Automatic discovery of SAN attached equipment. Must support various fabric switches regardless of vendor.

Interoperability - Management software must be listed as a Storage Networking Industry Association (SNIA) SMI-S 1.1 conforming client.
(http://www.snia.org/forums/smi/tech_programs/ctp/smi_conform/smi_client/smi_client_definitions

SAN Reporting - Automated reports of storage allocations must be capable of being generated by non-IT staff.

Proactive monitoring and remote notification - SAN Management software must be capable of monitoring and remote notification in the event of an alert, failure or the inability of the system to meet the customer's SLA's. Provisioning actions are required to trigger events, SNMP traps, and policies for notification. Must have the ability to send email, run customized scripts or programs for notifications.

Performance monitoring - Storage management software to monitor, analyze and report on all solution components (i.e. from host to fabric to storage). This includes storage subsystems, software operations, SAN infrastructure, replication and telecommunications. Software should be able to identify and analyze response time, and other relevant metrics to enable identification and resolution of potential bottlenecks.

Single SAN management console - Storage hardware must be manageable from a single storage management application.

Consistent design - All software should use identical components where possible to facilitate common updates across the solution.

EVALUATION FACTORS

- Enterprise Level Storage Management software
- Ability to manage multiple devices
- Enterprise License w/5years annual maintenance
- Storage Management Reporting
- Performance Monitoring
- Single Storage management console
- Ability to Manage events and policies

IMPLEMENTATION GUIDANCE

Implementation should include all optional software needed to meet the requirements listed above. Licensing and maintenance terms should the Hardware/Software Technical Support sections of this document. Professional implementation services should be included along with "classroom" training for support staff as outlined in the Training sections of this document.

3.4.4 [HARDWARE/SOFTWARE TECHNICAL SUPPORT]

STANDARD

ID	Secondary Attribute	Specification
	Support procedures	Documented support/escalation procedure for all components of the solution.
	Support Availability	Software support required 24x7x365 for all software provided in the solution. License and annual maintenance 3 years with 2 extension years.
		Hardware Maintenance/Support 5 yr, 24x7x365, 4 hour response time is required.
	License transfer	Licenses can be transferred without limitation within the Department of Veterans Affairs.
	OEM resources	Direct access to on-line OEM vendor support incident information and tracking.
	Support Interface	All VA datacenters must have access to incident information and tracking for all VA datacenters.
	Disruptive patches	Describe any type of updates/patch that would require a hosted service outage of the solution.
	SLAs	Documented Service Level Agreements (SLAs) for support requests.
	Professional services	Include cost of any professional services for services that must be completed by the vendor.

EXPLANATION OF STANDARD

Support procedures – A documented (digital & printed) set of instructions and escalation procedures to include updated contact information for the appropriate point of contact while troubleshooting problems. This will be a living document and as such digital copies should have supplements/replacements provided quarterly to ensure the most up to date procedures are available for the customer.

A concisely documented set of procedures is essential for communication between the customer and the support staff, allowing for all parties to know when priority escalation occurs, how it occurs, and the proper path for the expedited resolution.

Support Availability – Due to the criticality of these systems, full round the clock support is essential for a minimum of the first year, with options available to extend for the following four years allowing for a total of five years. In addition a minimal 4 hour response time in regards to hardware maintenance is required.

License transfer – All pertinent licenses must be capable of being transferred between various VA sites and cannot be restricted by location. Due to the nature of the OI&T structure for the VA licenses must be capable of being transferred within the various physical locations without restriction.

OEM resources – Direct communication paths to the knowledge experts of a product is key for fast response and ensuring the systems remain operational at the levels needed. Being required to go through middlemen in efforts to funnel trouble calls is not suitable to the nature of these systems.

Speaking directly with the product expert allows for potential miscommunication errors to be avoided. Being able to go directly to the appropriate level of tier knowledge on a failure is essential for ensuring that the problem is communicated correctly and quickly the best support engineer that can assist the customer.

Support interface – Due to many VA experts working across various regions and areas it is vital for all site's to be able to access VA wide information for troubleshooting and sharing of information.

VA I.T. support is organized through a central Office of Information Technology and is required to assist each various region/area as needed. Support contact and information should not be limited to a locality and must allow for access across the VA areas.

Disruptive patches – Ideally updates/patches will be able to be implemented with 0% system downtime. Any operations that would require a system outage needs to be documented and provided for review.

VA standards require that all disruptions be documented, submitted, and tracked to resolution. Known procedures that require disruption of service need to be documented and said documentation made available. Support engineers will need to work with VA staff to ensure that the required procedures for disruptions are followed.

SLAs - Documented Service Line Agreements (SLAs) for support request will be provided and the Vendor will ensure that there is no confusion between VA staff and Vendor on expectations.

Professional services – Provide a full disclosure of vendor specific services that must be provided by the vendor only. I.E. Some storage systems require a vendor engineer to flash firmware or similar upgrades and do not allow the customer to perform such actions.

VA standards require that outside contractors be escorted and/or evaluated for security requirements. All expected procedures that require vendor services need to be provided and a list of potential engineers that will be onsite updated as needed to ensure the engineer can gain access.

EVALUATION FACTORS

- Quality of documentation to include ease of finding information, extent of informative data, and usability in regards to trouble shooting and technical support will be considered.

- Direct phone contact for immediate escalation of troubleshooting over email, web interface, or other "automated" trouble shooting requests will be preferred.
- While direct access to product experts are needed, having a support engineer/contact to supervise and ensure that all experts are moving forward with the end goal of problem expedient problem resolution is preferred.
- Central/Single Interface for multiple sites to track VA related problems will be preferred.
- Minimum amount of scheduled downtime for patching/updating and supporting evidence for such is preferred.
- Path of communication for VA to suggest improvements and see improvements implemented is beneficial.
- Forums or other user group discussion areas are beneficial.
- Lower on-site response time is beneficial.
- Lower initial "engineer level" contact response time is beneficial.
- Lower time-to-repair is beneficial.
- Vendor-supplied components stocked as spares near, or at, facility is beneficial.
- Penalty clauses for vendor not meeting support contract provides is beneficial.

IMPLEMENTATION GUIDANCE

Coordination with initial VA staff for knowledge transfer and verified understanding is important. Continuing contact with VA staff to ensure support procedures are viable and procedures in place for VA input to improve support/product is essential.

3.4.5 [HARDWARE/SOFTWARE INSTALLATION]

STANDARD

ID	Secondary Attribute	Specification
	Installation	Provide hardware/software installation, including initial configuration, Storage Area Network configuration & knowledge transfer.
	Pre-configuration	Rack mount and configure the solution (including servers and storage where possible) prior to shipping it to the VA. This minimizes the on-site installation time as well as the number of crates and boxes that must be received and tracked by VA.
	Onsite impact	All on-site activities must be conducted in such a manner as to minimize the impact to normal information systems operations.
	Necessary software/hardware	Provide all necessary hardware and software, including all necessary cables and mounting hardware to make the Solution operational, except government-furnished property (GFP) referenced in GFP section.
	Necessary software/hardware	Provide inside delivery, installation and insurance of all equipment to VA datacenters. The VA does not accept delivery of the equipment until acceptance testing is passed at all VA datacenters.
	Trash	Remove all trash associated with shipping, delivery and installation.
	OS installation and security	Refer to Server Standard, Section Class C Server
	Single-initiator zoning	Hosts shall be connected using single-initiator zoning configuration.

EXPLANATION OF STANDARD

Installation - Provide planning, configuration and tentative schedule for the initial installation. This planning should involve collaborating with customer technical personnel to insure any and all critical elements and requirements regarding the environment are communicated. This process is envisioned as a collaborative effort between the vendor and customer with the end result being an installation that is 100 percent complete, functional and fully documented and the customer understanding everything needed to operate and maintain the system. This also includes demonstrating the steps necessary to backup and restore the system to a fully functional state. This entire process is to be conducted in such a manner as to minimize the impact to normal information systems operation.

Pre-configuration - To shorten the installation process and better utilize the time vendor personnel are on-site it is required pre-racking and pre-configuring the solution as much as possible prior to delivery. This includes working with customer personnel to develop any custom software images and preload the images prior to shipping.

Restorable images – In addition to having hardware preloaded with software a process must be in place to have restorable images for these systems as a backup to needing to overwrite/restore an existing image during install. Custom DVD's, portable storage, etc… are all viable options to having the image onsite for quick access and use.

Onsite impact – Minimal impact on the site facility is required. Efforts will be taken by the Vendor to ensure that the prep, assembly, install, and testing of the Solution will be done in a professional manner with minimal impact upon local site. Concern in regards to trash, path blockage, unsecured equipment, excessive levels of noise, etc… should be considered and action taken accordingly.

Necessary software/hardware – Aside from government-furnished property (GFP) referenced in the GFP section, all software and hardware required to make the Solution operational will be provided by the Vendor. This is to include but not limited to: cables, mounting brackets, screws, install software, testing equipment, etc…

Delivery – The Vendor will take responsibility of ensuring that all materials are delivered into the facility install location and the materials will remain the responsibility of the Vendor until acceptance testing is passed at all VA datacenters.

Trash – The Vendor will take responsibility of the removal of all trash from the facility, including but not limited to: boxes, packing materials, plastic bags, ties, etc…

OS installation and security – Following existing documentation provide by the VA Platform Server Team ensure all Operating systems and Security applications are installed accordingly.

Single-initiator Zoning – Best practices follow a Single-initiator zoning plan, keeping each host separate and easily managed as such. The solution needs to not only be capable of supporting Single-initiator zoning but restrictions on the number of zones should be minimal.

The reason is to avoid SCSI interrupt affecting from one host to another host. It is to isolate each device so that they do not affect each other.

EVALUATION FACTORS

- It is considered beneficial if the vendor can detail a delivery, installation and configuration plan for the equipment the vendor is proposing.
- Any demonstration that equipment can be pre-racked, pre-configured or pre-imaged is considered beneficial
- Verification that images can be restored onsite instead of remotely for install purposes is preferred.
- A basic plan to show minimal impact during installation and setup with a certified technicians to follow this plan is preferred. Vendor hiring lowest cost "IT Talent" is not preferred.
- Checklists of hardware and software installation needs and verified availability of these is beneficial.

IMPLEMENTATION GUIDANCE

As much Vendor/VA staff preinstall communication to ensure full understanding is recommended.

Vendor verification of hardware fitting and requirements prior to install is required. Finding out at install that a piece of equipment does not fit or does not have all the install equipment is not acceptable.

All documentation, software, and hardware required for installation and operation of the Solution as well as training materials need to be onsite and verified for installation.

3.4.6 [TRAINING]

STANDARD

ID	Secondary Attribute	Specification
	Training Length	Provide equivalent of one day of certified vendor classroom training for every 24 fiber channel ports provided.
	Knowledge transfer	Work with VA staff as activities occur to ensure that VA can assume operational responsibility for the delivered solution.
	Documentation	Provide electronic copies of all materials, manuals, worksheets, etc. used in the delivery of the solution.

EXPLANATION OF STANDARD

Training Length – An initial complete training for VA staff is important for this project to succeed. An equivalent of one day of certified vendor classroom training for every 24 fiber channel ports, or more if the vendor believes this is needed.

VA support staff must have a level of trained knowledge provided to allow them to operate at a high level of expertise for day to day operations and standard problem resolution.

Knowledge transfer – While classroom training is important for the understanding of principles and procedures, actual knowledge transfer in regards to the implemented packages, how they work in the VA environment and potential improvement that may be available or upcoming is required.

Documentation – Initially all documentation for training, materials, worksheets, etc… for the initial installation must be provided in electronic format to ensure standard knowledge for all VA staff. As the product is changed and improved future training and documentation will also need to be provided.

Training documentation must be as complete as possible to allow for new VA staff to be able to understand and work with the vendor product.

EVALUATION FACTORS

- Vendor specific training that is oriented towards certification or “engineer” level training that is pertinent to properly managing and troubleshooting the product is preferred.
- Additional time/effort spent working with VA staff to ensure that the VA environment is optimized and meeting VA expectations is beneficial.
- When directly training VA staff printed as well as digital materials is beneficial to allow full potential of learning from staff.
- User forums for exchange of ideas and knowledge are preferred.

IMPLEMENTATION GUIDANCE

Any implementation that requires a strong base of knowledge for VA staff needs to have a planned training event set in place prior to installation to allow for full VA understanding and best potential for project implementation. While this training should be prior to installation it must not be so far in advance that newly learned skills/knowledge will become stale/obsolete by installation time.

In addition any installation that will occur near a time of a new patch or revision needs to ensure that the new knowledge is provided with the training.

3.5 [GENERAL BACKUP AND ARCHIVE STANDARD]

3.5.1 [BACKUP METHOD]

STANDARD

ID	*Secondary Attribute*	*Specification*
	Tape	Direct tape backup from Primary storage
		Snapshot from Primary disk to secondary disk and backup to tape. Offload backup resources from primary storage device to secondary storage device (VTL or disk) is preferred
	Disk (Tapeless)	Backup from Primary disk to secondary disk such as Virtual tape library (VTL) with deduplication solution that meets all other backup requirements including retention and offsite storage policy
		Continuous Data Protection (CDP) is preferred for stringent SLA, RPO, and RTO requirements and the ability to recover ANY point in time
		Support Asynchronous replication with deduplicated data is preferred.
	Archive	Long term Data Archiving solution must meet OGC VA Litigation, State, and Federal requirements
		For data not access frequently

EXPLANATION OF STANDARD

TAPE

- Direct tape backup from Primary Storage – The ability to utilize direct tape backup from primary storage is for compliance with government regulations which requires full monthly data backup to an offsite tape location.

- Snapshot from Primary Disk to secondary disk and backup to tape. Offload backup resources from primary storage device to secondary storage device (VTL or disk) is preferred. - Due to the compliance with government regulation which include; Sarbanes-Oxley Act (2002) intended to "deter and punish corporate and accounting fraud and corruption, ensure justice for wrongdoers, and protect the interest of workers and shareholders" (President Bush), USA Patriot Act passed in September of 2001 which introduced a plethora of legislative changes that significantly increased the surveillance and investigative powers of law enforcements agencies in the US., and the Health Insurance Portability and Accountability Act (HIPPA) of 1996 involves legislation protecting patient privacy and records security – organizations are required to store, manage, and safeguard a lot more data. This has lead to the need for more storage capacity and more efficient methods of backing up, retrieving, and archiving data. Snapshot from Primary Disk to secondary disk and backup to tape is one way to

effectively accomplish a proper protection and recovery strategy of large data sets and still meet the tape backup compliance required by government regulations. This method offloads backup process from primary storage to secondary storage to allow wider backup windows that are not restricted by the production hours.

Disk (Tapeless)

- Backup from Primary disk to secondary disk such as Virtual tape library (VTL) with deduplication solution that meets all other backup requirements including retention and offsite storage policy. – Disk based backup is a solution to effectively meet the backup window requirements of the data center. The backups are faster, restores are more reliable. If you incorporate a VTL into the environment, you can reference physical disk as a VTL allowing the backup software to see the VTL as a tape drive. You can also include data deduplication technologies. Data deduplication systems employ a data reduction technique that identifies common "chunks" of bytes among multiple data files, and only stores these chunks once. Using this method allows you to store data in less disk space.

- Continuous Data Protection (CDP) is preferred for stringent SLA, RPO, and RTO requirements and the ability to recover ANY point in time. – Continuous Data Protection (also known as synchronous replication) is a backup and recovery solution that continuously backs up data as it changes to ensure recovery of a current version within minutes of a failure. The data is always current between the sites but is a more expensive solution than asynchronous.

- Support Asynchronous replication with deduplicated data is preferred. - With asynchronous replication, there is a delay before the data gets written to the secondary site. Because asynchronous replication is designed to work over distances and requires less bandwidth, it is often a better option for disaster recovery. However, asynchronous replication risks a loss of data during a system outage because data at the target device is not up to date with the source data. Data deduplication is often combined with replication for disaster recovery purposes. Deduplication reduces the amount of data that gets replicated and lowers the bandwidth requirement to copy data to secondary site.

Archive

- Long term Data Archiving solution must meet with OGC VA Litigation, State, and Federal requirements. – Federal and state laws, including Health Insurance Portability and Accountability Act (HIPAA) regulations, require covered entities to store certain data, such as the final, consolidated, electronic version of a Patient Medical Record, for up to 75 years after the last episode of patient care. More information can be found in the website http://vista.med.va.gov/iss/ . In addition, long term Data Archiving solution is needed based on the guidelines Litigation Hold Memo Appendix A 6-30-08.pdf dated 6-30-2008 referenced on the Office of General Counsel – OGC VA Litigation website, http://vaww.client.gc.va.gov/General/Litigation/vcs/index.htm .

- For data not access frequently – When infrequently accessed files are stored, they consume ever increasing amounts of storage space and cause daily backups to increase. Data Archiving moves the files from expensive disk storage to less expensive media, but allows information to be always available. For business, legal, and regulatory requirements, the data must be available for many years or even decades.

EVALUATION FACTORS

- Lowest Total Cost of Ownership (TCO) solution that meets the performance requirements is preferred. Components considered are small footprint, power consumption, cooling, Hardware, Software, license, Overhead cost of managing the devices, Ease of Management, Acquisition cost, Maintenance and deployment costs, storage capacity (such as number of data copies),Information Lifecycle Management(ILM) cost.
- Disk (Tapeless)/Archive – It is beneficial to be able to have VTL and Archive storage resides in one storage device.
- Avoid products with proprietary Application Programming Interface (API) that only allow its product to store or recover data.

IMPLEMENTATION GUIDANCE

Lowest Total Cost of Ownership (TCO) solution that meets the performance requirements is preferred.

Create snapshots or clones to secondary disks are recommended.

Offload direct tape backup process from primary disks is recommended as it will have less impact to production performance and eliminates the backup window restriction.

Ensure solution has alternate way to store and retrieve data locally or remotely.

Implement Asynchronous replication with deduplicated data. Global deduplication among multiple devices is recommended.

3.5.2 [VIRTUAL TAPE LIBRARY (VTL) HARDWARE]

STANDARD

ID	Secondary Attribute	Specification
	Technology	Support Massive Array of Idle Disks (MAID)
	Disk health monitoring	Capable of pro-actively disks monitoring and detecting potential drive failures before it occurs.
	Deduplication	Minimum of supporting post process data deduplication.
	Replication	Support Asynchronous replication with deduplicated data
	Raw Storage Capacity	Up to 896 TB per cabinet
	Number of Emulated Tape Libraries	1 to 8
	Number of Emulated Tape Drives	1 to 28 standard (1-512 with HPCM option)
	Number of Virtual Tape Cartridges	Up to 8192
	Connectivity	Minimum four FC connectivity of 4 GigE ports per system.
	Redundancy	Redundant fan, N+1 Redundancy, Hot-Swappable Power Supplies

EXPLANATION OF STANDARD

Technology – MAID (massive array of idle disks) is a storage technology that employs a large group of disk drives in which only those drives in active use are spinning at any given time. This reduces power consumption and prolongs the life of the drives. MAID is designed for Write Once Read Occasionally (WORO) applications. The disk spin down feature of the MAID technology allows cost savings from bulk purchase of disks in the initial procurement. Disks that are not used are spin down that save energy cost and disk access life; and only spin up when it is used.

Disk health monitoring - Capable of pro-actively monitor the health of disks by performing integrity checks on all disks. Capable of copy data from a potentially failing disk to a new healthy spare disk, avoiding lengthy RAID rebuild times and data loss.

Deduplication – Data Deduplication is a technology strives to reduce the amount of duplicate data being backed up and then stored. The technologies identify and eliminate common data in and across backup streams. By eliminating the common objects, the resulting storage requirement will be reduced.

Global deduplication comes into play when you have multiple deduplication devices. With multiple deduplication devices nodes, when data that is seen before by one node is sent to a second node, the second node knows that data has already been stored and it will not be stored for a second time.

Replication - Replication is typically a software function, but hardware must support replication.

Raw Storage Capacity – Specification from market research needed for Enterprise Class Data Center environment.

Number of Emulated Tape Libraries – Specification from market research needed for Enterprise Class Data Center environment.

Number of Emulated Tape Drives – Specification from market research needed for Enterprise Class Data Center environment.

Number of Virtual Tape Cartridges – Specification from market research needed for Enterprise Class Data Center environment.

Connectivity – Storage subsystem must have multiple 4 Gb/second connectivity. An 8/GB connection is highly desirable.

Redundancy – Failure of a single component will not stop storage system operation in any capacity. Fully redundant storage systems are critical to the continuing processing and to maintain system stability.

EVALUATION FACTORS

- Lowest Total Cost of Ownership (TCO) solution that meets the performance requirements is preferred. Components considered are small footprint, power consumption, cooling, Hardware, Software, license, Overhead cost of managing the devices, Ease of Management, Acquisition cost, Maintenance and deployment costs, storage capacity (such as number of data copies),Information Lifecycle Management(ILM) cost.
- Redundant components are needed to ensure the failure of one component of the storage system will not cause an outage.
- Using the same replication software for Primary storage and all other storage is beneficial.
- It is beneficial to be able to have VTL and Archive storage resides in one storage device.
- Deduplication – Source, target, inline, or post process deduplication. The deduplication method used must not degrade overall application performance, storage performance, and will not reduce backup windows. Support Global deduplication is preferred.
- Capable of perform both file-level, and block-level data deduplication is preferred.
- Capable of perform both file-level and block-level data deduplication on primary storage is preferred.
- Avoid products with proprietary Application Programming Interface (API) that only allow its product to store or recover data.

IMPLEMENTATION GUIDANCE

Lowest Total Cost of Ownership (TCO) solution that meets the performance requirements is preferred.

Offload direct tape backup process from primary disks is recommended as it will have less impact to production performance and eliminates the backup window restriction.

Ensure solution has alternate way to store and retrieve data locally or remotely.

Redundancy **–** Include validation in acceptance testing**.** Component failure testing should occur prior to putting into production. This should include a planned failure of a single component to ensure the backup/ secondary component provides adequate coverage to verify no outage of the storage system.

Deduplication – Must test and validate to ensure the deduplication method used does not degrade overall application performance, storage performance, and will not reduce backup windows. Test and validate to ensure Global deduplication only process one copy of data among sites.

Implement Asynchronous replication with deduplicated data. Global deduplication among multiple devices is recommended.

3.5.3 [ARCHIVE HARDWARE]

STANDARD

ID	Secondary Attribute	Specification
	Technology	Support Massive Array of Idle Disks (MAID)
	Disk health monitoring	Capable of pro-actively disks monitoring and detecting potential drive failures before it occurs.
	Data Storage Architecture	Support write-once-read-many (WORM) and Write Once Read Occasionally (WORO)
	Deduplication	Minimum of supporting post process deduplication.
	Replication	Support Asynchronous replication with deduplicated data
	Protocol Support	CIFS,NFS V2 + V3, TCP/IP
	Number of Files	Up to 1.5 Billion files
	File Size	Up to 1.2TB file size
	Raw Storage Capacity	Up to 896 TB per cabinet
	Number of drives	Single Cabinet Up to 896 drives
	Connectivity	Minimum four FC connectivity of 4 GigE ports per system
	Redundancy	Redundant fan, N+1 Redundancy, Hot-Swappable Power Supplies

EXPLANATION OF STANDARD

Technology – MAID (massive array of idle disks) is a storage technology that employs a large group of disk drives in which only those drives in active use are spinning at any given time. This reduces power consumption and prolongs the life of the drives. MAID is designed for Write Once Read Occasionally (WORO) applications. The disk spin down feature of the MAID technology allows cost savings from bulk purchase of disks in the initial procurement. Disks that are not used are spin down that save energy cost and disk access life; and only spin up when it is used.

Disk health monitoring - Capable of pro-actively monitor the health of disks by performing integrity checks on all disks. Capable of copy data from a potentially failing disk to a new healthy spare disk, avoiding lengthy RAID rebuild times and data loss.

Data Storage Architecture – In order to reduces power consumption and prolongs the life of the drives. The system is capable of supporting Write Once Read Occasionally (WORO). For security application, the system is capable of supporting Write Once Read Many (WORM) storage Data Storage Architecture.

Deduplication – Data Deduplication is a technology strives to reduce the amount of duplicate data being backed up and then stored. The technologies identify and eliminate common data in and across backup streams. By eliminating the common objects, the resulting storage requirement will be reduced.

Global deduplication comes into play when you have multiple deduplication devices. With multiple deduplication devices nodes, when data that is seen before by one node is sent to a second node, the second node knows that data has already been stored and it will not be stored for a second time.

Protocol Support - Product that supports common protocol like NSF and CIFS is required. Avoid product with proprietary Application Programming Interface (API) that only allow its product to store or recover data.

Replication - Replication is typically a software function, but hardware must support replication Protocol Support.

Number of Files - Specification from market research needed for Enterprise Class Data Center environment.

File Size - Specification from market research needed for Enterprise Class Data Center environment.

Raw Storage Capacity - Specification from market research needed for Enterprise Class Data Center environment.

Number of drives - Specification from market research needed for Enterprise Class Data Center environment.

Connectivity – Storage subsystem must have multiple 4 Gb/second connectivity. An 8/GB connection is highly desirable.

Redundancy – Failure of a single component will not stop storage system operation in any capacity. Fully redundant storage systems are critical to the continuing processing and to maintain system stability.

EVALUATION FACTORS

- Lowest Total Cost of Ownership (TCO) solution that meets the performance requirements is preferred. Components considered are small footprint, power consumption, cooling, Hardware, Software, license, Overhead cost of managing the devices, Ease of Management, Acquisition cost, Maintenance and deployment costs, storage capacity (such as number of data copies),Information Lifecycle Management(ILM) cost.
- Redundant components are needed to ensure the failure of one component of the storage system will not cause an outage.
- Using the same replication software for Primary storage and all other storage is beneficial.
- It is beneficial to be able to have VTL and Archive storage resides in one storage device.
- Deduplication – Source, target, inline, or post process deduplication. The deduplication method used must not degrade overall application performance, storage performance, and will not reduce backup windows. Support Global deduplication is preferred.
- Capable of perform both file-level, and block-level data deduplication is preferred.
- Capable of perform both file-level and block-level data deduplication on primary storage is preferred.
- Avoid products with proprietary Application Programming Interface (API) that only allow its product to store or recover data.

IMPLEMENTATION GUIDANCE

Lowest Total Cost of Ownership (TCO) solution that meets the performance requirements is preferred.

Ensure solution has alternate way to store and retrieve data locally or remotely.

Redundancy **–** Include validation in acceptance testing**.** Component failure testing should occur prior to putting into production. This should include a planned failure of a single component to ensure the backup/ secondary component provides adequate coverage to verify no outage of the storage system.

Deduplication – Must test and validate to ensure the deduplication method used does not degrade overall application performance, storage performance, and will not reduce backup windows. Test and validate to ensure Global deduplication only process on copy of data among sites.

Implement Asynchronous replication with deduplicated data. Global deduplication among multiple devices is recommended.

3.5.4 [TAPE LIBRARY HARDWARE]

STANDARD

ID	Secondary Attribute	Specification
	Interoperability - Industry standards	Tape Library must provide for tape drives with minimum 800 GB uncompressed and throughput minimum of 120 MB/sec. Tape Library drives must be capable of encryption with minimum 1TB tape capacity and throughput minimum of 120 MB/sec. (FIPS 140-2, Level 3)
	Compatibility	Tape library must be capable of reading previously written tapes in the following formats: DLT and LTO.
	Backup SAN	Solution must provision SAN/network components as required to meet performance requirements and isolate backup traffic from normal production traffic.
	Connectivity	Fiber Channel, FICON, ESCON
	Fully redundant configuration	Provide fully redundant configuration such as ports, robots, tape drives, power supplies.
	Current generation equipment	Tape libraries and/or components must not be listed on vendor websites as “end of life” or “end of sale”. The initial hardware general availability date should be less than 5 years from the proposal submission date.
	Library Capacity (throughput)	Minimum throughput of 16 TB per hour
	Capacity (slots)	Solution must provide a minimum of 500 active tape slots
	Scalability (throughput)	Minimum scalability of 20 TB per hour
	Scalability (slots)	Solution must provide the ability to expand to 100% of minimum number of tape slots.
	Rack Configuration	Provide appropriate 4 posts (42 or 47 U) with sidewalls.
	Manageable power supplies	Redundant IP Manageable & Accessible Power Distribution Unit (PDUs) sufficient to power all units in the rack.

	Cooling	N + 1 Fans to support airflow requirements.
	Physical layout	All components must be easily accessible without having to de-install, disconnect or remove other components so that service can be easily accomplished.
	Size	Equipment footprint of less than 60 square feet in fully-scaled configuration.
	Standardized layouts	Components must be mounted in standardized configurations for all VA installations.
	Additional servers	Refer to Server Standard, Section Class C Server.
	Online maintenance	Ability to make hardware changes, repairs and expansion without impacting daily operations.

EXPLANATION OF STANDARD

Interoperability - Industry standards - for consistency and to ensure that the tape library provided meets the criteria set forth by both Industry Standards and the VA Standard a baseline of specifications are needed. These specifications are best indicated by the Storage Management Initiative Specification (SMI-S) which was developed by leading storage equipment and software providers.

Compatibility - Tape library must be capable of running multiple formats of tape drives in a single tape library in order to read previously written tapes. Minimum supported formats are DLT and LTO.

Backup SAN – It is preferred to have a dedicated SAN for backup traffic to reduce the impact of production performance. Backup traffic should be isolated from normal production LAN traffic.

Connectivity – Tape library must support a minimum of Fiber Channel, FICON, ESCON connectivity. Tape library must have minimum of supporting 4 Gb/second FC connectivity. An 8/GB FC connection is highly desirable.

Fully redundant configuration - Failure of a single component will not stop storage system operation in any capacity. Fully redundant system is critical to the continuing processing and to maintain system stability.

Current Generation Equipment - Tape libraries and/or components must not be listed on vendor websites as “End of Life” , “End of Sale” or ”End of Service Life”. The initial hardware general availability date should be less than 5 years from the proposal submission date.

Library Capacity (throughput) - Specification from market research needed for Enterprise Class Data Center environment.

Capacity (slots) - Specification from market research needed for Enterprise Class Data Center environment.

Scalability (throughput) - Specification from market research needed for Enterprise Class Data Center environment.

Scalability (slots) - Specification from market research needed for Enterprise Class Data Center environment.

Rack Configuration - Provide appropriate 4 posts (42 or 47 U) with sidewalls as specified by VA requirements

Manageable Power Supplies – Ability to manage thru an API or other standard interface from a remote location all power metrics of the PDU's.

Cooling – Tape library must be able to lose one fan without causing an outage or cause the system to be unstable.

Physical Layout – All components must be easily accessible without having to de-install, disconnect or remove other components so that service can be easily accomplished.

Size - Specification from market research needed for Enterprise Class Data Center environment.

Standardized layouts - The layout of the solution must be a consistent design that is in use at all datacenters that are keeping with VA standards. This approach allows for the redistribution of the equipment to different sites and the most efficient use of data center space.

Additional Servers – Refer to Server Standards, Section Class C Server.

Online maintenance - Ability to make hardware changes, repairs and expansion without shutting down the tape library system. The system has the ability to allow hot swapping of its hardware components, dynamic update of its firmware and software.

EVALUATION FACTORS

- Lowest Total Cost of Ownership (TCO) solution that meets the performance requirements is preferred. Components considered are small footprint, power consumption, cooling, Hardware, Software, license, Overhead cost of managing the devices, Ease of Management, Acquisition cost, Maintenance and deployment costs, storage capacity (such as number of data copies),Information Lifecycle Management(ILM) cost.
- **Interoperability – Industry standards** – REQUIRED the supporting documentation should be presented and validated during the acquisition process. These specifications are SMI-S v1.1 as described at: http://www.snia.org/forums/smi/tech_programs/smis_home/
- Tape Library drives must be capable of encryption. Both hardware and key management system must comply with FIPS 140-2 level 3 standards.
- **Compatibility** - Tape library must be capable of running multiple formats of tape drives in a single tape library.
- **Connectivity** – Tape library must have minimum of supporting 4 Gb/second FC connectivity. An 8/GB FC connection is highly desirable.
- Redundant components are needed to ensure the failure of one component of the tape system will not cause an outage.

IMPLEMENTATION GUIDANCE

Lowest Total Cost of Ownership (TCO) solution that meets the performance requirements is preferred.

Offload direct tape backup process from primary disks is recommended as it will have less impact to production performance and eliminates the backup window restriction.

Ensure solution has alternate way to store and retrieve data locally or remotely.

Interoperability – Industry standards - The standards which are provided in the sections above must be adhered to and validated during the implementation phase using the common set of tools identified in the SMI-S v1.1.

Backup SAN – Tape library should have dedicated SAN to isolate Backup traffic from normal production LAN traffic.

Redundancy **i**ncludes validation in acceptance testing**.** Component failure testing should occur prior to putting into production. This should include a planned failure of a single component to ensure the backup/ secondary component provides adequate coverage to verify no outage of the tape system.

Standardized layouts - Ensure that all layouts conform to VA Standard and are validated during installation.

3.5.5 [BACKUP SOFTWARE/VTL/ARCHIVE/TAPE LIBRARY TOOL]

STANDARD

ID	Secondary Attribute	Specification
	Backup Software	Provide Enterprise level backup software with ODBC and JDBC connectivity.
		Support Open VMS client and Open VMS Scripting is required
		Software with source and target Deduplication capability. Support Global Deduplication is preferred.
		Capable of synthetic backup
		NDMP backup and restore capable of performing block level backup and file level restore
		Capable of creating snapshots and clones. Support Continuous Data Protection (CDP)
	Tape Library management tool	Provide Enterprise level Tape Library management software. Compatibility with tape backup software. Listed on the VA Technical Reference Model (TRM) is preferred
	Encryption	Enterprise Backup software encryption and Enterprise encryption key management system complying with FIPS 140-2 level 3 standards without regard to application, operating system or primary storage device.
	Compatibility	Compatibility with operating systems listed on the VA Technical Reference Model (TRM)
	Scripting	Compatibility with operating systems listed on the VA Technical Reference Model (TRM)
	Proactive monitoring and remote notification	The software and management tool must be capable of proactive monitoring and remote notification of system and application health. Must support ODBC and/or JDBC connectivity.
	Role-based access	Solution must include security configurations that support role-based access required to limit functions during normal and COOP operation.

	Manageability	Manageable from a single application provided as part of the solution.
	Additional servers	Refer to Server Standard, Section Class C Server.
	Management server security	Refer to Server Standard, Section Class C Server.
	Consistent design	All software should use identical components where possible to facilitate common updates across the solution.

EXPLANATION OF STANDARD

Backup Software - Provide Enterprise level backup software with ODBC and JDBC connectivity. Must support Open VMS (**Open Virtual Memory System**), client and Open VMS (**Open Virtual Memory System**), Scripting. Software with source and target Deduplication capability. Support Global Deduplication (*DATA DEDUPLICATION WHICH REMOVES DUPLICATE DATA ACROSS MULTIPLE DEDUPLICATION SYSTEMS*) is preferred. Capable of synthetic backup(full and subsequent incremental backups). NDMP ***(Network Data Management Protocol)*** backup and restore capable of performing block level backup and file level restore. Capable of creating snapshots and clones with support for Continuous Data Protection (CDP).

Tape Library management tool - Provide Enterprise level Tape Library management software. Compatibility with tape backup software. Listed on the VA Technical Reference Model (TRM) is preferred.

Encryption - Enterprise Backup software encryption and Enterprise encryption key management system complying with FIPS 140-2 level 3 standards without regard to application, operating system or primary storage device.

Compatibility - Compatibility with operating systems listed on the VA Technical Reference Model (TRM)

Scripting - Compatibility with operating systems listed on the VA Technical Reference Model (TRM)

Proactive monitoring and remote notification - Backup software must be capable of monitoring and remote notification in the event of an alert, failure or the inability of the system to meet the customer's SLA's. Ability to send email or custom scripts or programs for notification.

Role-based access - Solution must include security configurations that support role-based access required to limit functions during normal and COOP(Continuity of Operations) operation.

Manageability - Manageable from a single application provided as part of the solution.

Consistent design - All software should use identical components where possible to facilitate common updates across the solution.

EVALUATION FACTORS

- Open VMS Support
- Continuous Data Protection

- Block Level Backups
- Snap shot capabilities
- Clone capabilities
- Remote Notification
- Scripting capabilities
- Encryption capabilities with FIPS 140-2 support

IMPLEMENTATION GUIDANCE

Implementation should include all optional software needed to meet the requirements listed above. Licensing and maintenance terms should the Hardware/Software Technical Support sections of this document. Professional implementation services should be included along with "classroom" training for support staff as outlined in the Training sections of this document.

3.5.6 [HARDWARE/SOFTWARE TECHNICAL SUPPORT]

STANDARD

ID	Secondary Attribute	Specification
	Support procedures	Documented support/escalation procedure for all components of the solution.
	Support Availability	Software support required 24x7x365 for all software provided in the solution. License and annual maintenance 3 years with 2 extension years.
		Hardware Maintenance/Support 5 yr, 24x7x365, 4 hour response time is required .
	License transfer	Licenses can be transferred without limitation within the Department of Veterans Affairs.
	OEM resources	Direct access to on-line OEM vendor support incident information and tracking.
	Support Interface	All VA datacenters must have access to incident information and tracking for all VA datacenters.
	Disruptive patches	Describe any type of updates/patch that would require a hosted service outage of the solution.
	SLAs	Documented Service Level Agreements (SLAs) for support requests.
	Professional services	Include cost of any professional services for services that must be completed by the vendor.

EXPLANATION OF STANDARD

Support procedures – A documented (digital & printed) set of instructions and escalation procedures to include updated contact information for the appropriate point of contact while troubleshooting problems. This will be a living document and as such digital copies should have supplements/replacements provided quarterly to ensure the most up to date procedures are available for the customer.

A concisely documented set of procedures is essential for communication between the customer and the support staff, allowing for all parties to know when priority escalation occurs, how it occurs, and the proper path for the expedited resolution.

Support Availability – Due to the criticality of these systems, full round the clock support is essential for a minimum of the first year, with options available to extend for the following four years allowing for a total of five years. In addition a minimal 4 hour response time in regards to hardware maintenance is required.

License transfer – All pertinent licenses must be capable of being transferred between various VA sites and cannot be restricted by location. Due to the nature of the OI&T structure for the VA licenses must be capable of being transferred within the various physical locations without restriction.

OEM resources – Direct communication paths to the knowledge experts of a product is key for fast response and ensuring the systems remain operational at the levels needed. Being required to go through middlemen in efforts to funnel trouble calls is not suitable to the nature of these systems.

Speaking directly with the product expert allows for potential miscommunication errors to be avoided. Being able to go directly to the appropriate level of tier knowledge on a failure is essential for ensuring that the problem is communicated correctly and quickly the best support engineer that can assist the customer.

Support interface – Due to many VA experts working across various regions and areas it is vital for all site's to be able to access VA wide information for troubleshooting and sharing of information.

VA I.T. support is organized through a central Office of Information Technology and is required to assist each various region/area as needed. Support contact and information should not be limited to a locality and must allow for access across the VA areas.

Disruptive patches – Ideally updates/patches will be able to be implemented with 0% system downtime. Any operations that would require a system outage needs to be documented and provided for review.

VA standards require that all disruptions be documented, submitted, and tracked to resolution. Known procedures that require disruption of service need to be documented and said documentation made available. Support engineers will need to work with VA staff to ensure that the required procedures for disruptions are followed.

SLAs - Documented Service Line Agreements (SLAs) for support request will be provided and the Vendor will ensure that there is no confusion between VA staff and Vendor on expectations.

Professional services – Provide a full disclosure of vendor specific services that must be provided by the vendor only. I.E. Some storage systems require a vendor engineer to flash firmware or similar upgrades and do not allow the customer to perform such actions.

VA standards require that outside contractors be escorted and/or evaluated for security requirements. All expected procedures that require vendor services need to be provided and a list of potential engineers that will be onsite updated as needed to ensure the engineer can gain access.

EVALUATION FACTORS

- Quality of documentation to include ease of finding information, extent of informative data, and usability in regards to trouble shooting and technical support will be considered.

- Direct phone contact for immediate escalation of troubleshooting over email, web interface, or other "automated" trouble shooting requests will be preferred.
- While direct access to product experts are needed, having a support engineer/contact to supervise and ensure that all experts are moving forward with the end goal of problem expedient problem resolution is preferred.
- Central/Single Interface for multiple sites to track VA related problems will be preferred.
- Minimum amount of scheduled downtime for patching/updating and supporting evidence for such is preferred.
- Path of communication for VA to suggest improvements and see improvements implemented is beneficial.
- Forums or other user group discussion areas are beneficial.
- Lower on-site response time is beneficial.
- Lower initial "engineer level" contact response time is beneficial.
- Lower time-to-repair is beneficial.
- Vendor-supplied components stocked as spares near, or at, facility is beneficial.
- Penalty clauses for vendor not meeting support contract provides is beneficial.

IMPLEMENTATION GUIDANCE

Coordination with initial VA staff for knowledge transfer and verified understanding is important. Continuing contact with VA staff to ensure support procedures are viable and procedures in place for VA input to improve support/product is essential.

3.5.7 [HARDWARE/SOFTWARE INSTALLATION]

STANDARD

ID	Secondary Attribute	Specification
	Installation	Provide hardware/software installation, including initial configuration, Storage Area Network configuration & knowledge transfer.
	Pre-configuration	Rack mount and configure the solution (including servers and storage where possible) prior to shipping it to the VA. This minimizes the on-site installation time as well as the number of crates and boxes that must be received and tracked by VA.
	Onsite impact	All on-site activities must be conducted in such a manner as to minimize the impact to normal information systems operations.
	Necessary software/hardware	Provide all necessary hardware and software, including all necessary cables and mounting hardware to make the Solution operational, except government-furnished property (GFP) referenced in GFP section.
	Delivery	Provide inside delivery, installation and insurance of all equipment to VA datacenters. The VA does not accept delivery of the equipment until acceptance testing is passed at all VA datacenters.
	Trash	Remove all trash associated with shipping, delivery and installation.
	OS installation and security	Refer to Server Standard, Section Class C Server.

EXPLANATION OF STANDARD

Installation - Provide planning, configuration and tentative schedule for the initial installation. This planning should involve collaborating with customer technical personnel to insure any and all critical elements and requirements regarding the environment are communicated. This process is envisioned as a collaborative effort between the vendor and customer with the end result being an installation that is 100 percent complete, functional and fully documented and the customer understanding everything needed to operate and maintain the system. This also includes demonstrating the steps necessary to backup and restore the system to a fully functional state. This entire process is to be conducted in such a manner as to minimize the impact to normal information systems operation.

Pre-configuration - To shorten the installation process and better utilize the time vendor personnel are on-site it is required pre-racking and pre-configuring the solution as much as possible prior to delivery. This includes working with customer personnel to develop any custom software images and preload the images prior to shipping.

Restorable images – In addition to having hardware preloaded with software a process must be in place to have restorable images for these systems as a backup to needing to overwrite/restore an existing image during install. Custom DVD's, portable storage, etc… are all viable options to having the image onsite for quick access and use.

Onsite impact – Minimal impact on the site facility is required. Efforts will be taken by the Vendor to ensure that the prep, assembly, install, and testing of the Solution will be done in a professional manner with minimal impact upon local site. Concern in regards to trash, path blockage, unsecured equipment, excessive levels of noise, etc… should be considered and action taken accordingly.

Necessary software/hardware – Aside from government-furnished property (GFP) referenced in the GFP section, all software and hardware required to make the Solution operational will be provided by the Vendor. This is to include but not limited to: cables, mounting brackets, screws, install software, testing equipment, etc…

Delivery – The Vendor will take responsibility of ensuring that all materials are delivered into the facility install location and the materials will remain the responsibility of the Vendor until acceptance testing is passed at all VA datacenters.

Trash – The Vendor will take responsibility of the removal of all trash from the facility, including but not limited to: boxes, packing materials, plastic bags, ties, etc…

OS installation and security – Following existing documentation provide by the VA Platform Server Team ensure all Operating systems and Security applications are installed accordingly.

EVALUATION FACTORS

- It is considered beneficial if the vendor can detail a delivery, installation and configuration plan for the equipment the vendor is proposing.
- Any demonstration that equipment can be pre-racked, pre-configured or pre-imaged is considered beneficial
- Verification that images can be restored onsite instead of remotely for install purposes is preferred.
- A basic plan to show minimal impact during installation and setup with certified technicians to follow this plan is preferred. Vendor hiring lowest cost "IT Talent" is not preferred.
- Checklists of hardware and software installation needs and verified availability of these is beneficial.

IMPLEMENTATION GUIDANCE

As much Vendor/VA staff preinstall communication to ensure full understanding is recommended.

Vendor verification of hardware fitting and requirements prior to install is required. Finding out at install that a piece of equipment does not fit or does not have all the install equipment is not acceptable.

All documentation, software, and hardware required for installation and operation of the Solution as well as training materials need to be onsite and verified for installation.

3.5.8 [TRAINING]

STANDARD

ID	Secondary Attribute	Specification
	Training Length	Provide equivalent of one day of certified vendor classroom training for every installed tape drive or every 12TB of VTL and Archive storage space.
	Knowledge transfer	Work with VA staff as activities occur to ensure that VA can assume operational responsibility for the delivered solution.
	Documentation	Provide electronic copies of all materials, manuals, worksheets, etc. used in the delivery of the solution.

EXPLANATION OF STANDARD

Training Length – An initial complete training for VA staff is important for this project to succeed. An equivalent of one day of certified vendor classroom training for every installed tape drive or every 12TB of VTL and Archive storage space, or more if the vendor believes this is needed.

VA support staff must have a level of trained knowledge provided to allow them to operate at a high level of expertise for day to day operations and standard problem resolution.

Knowledge transfer – While classroom training is important for the understanding of principles and procedures, actual knowledge transfer in regards to the implemented packages, how they work in the VA environment and potential improvement that may be available or upcoming is required.

Documentation – Initially all documentation for training, materials, worksheets, etc… for the initial installation must be provided in electronic format to ensure standard knowledge for all VA staff. As the product is changed and improved future training and documentation will also need to be provided.

Training documentation must be as complete as possible to allow for new VA staff to be able to understand and work with the vendor product.

EVALUATION FACTORS

- Vendor specific training that is oriented towards certification or “engineer” level training that is pertinent to properly managing and troubleshooting the product is preferred.
- Additional time/effort spent working with VA staff to ensure that the VA environment is optimized and meeting VA expectations is beneficial.
- When directly training VA staff printed as well as digital materials is beneficial to allow full potential of learning from staff.
- User forums for exchange of ideas and knowledge are preferred.

IMPLEMENTATION GUIDANCE

Any implementation that requires a strong base of knowledge for VA staff needs to have a planned training event set in place prior to installation to allow for full VA understanding and best potential for project implementation. While this training should be prior to installation it must not be so far in advance that newly learned skills/knowledge will become stale/obsolete by installation time.

In addition any installation that will occur near a time of a new patch or revision needs to ensure that the new knowledge is provided with the training.

4 TAXONOMY OF STANDARDS

A. Taxonomy of Tier1 Storage Standards, the followings are primary and secondary attributes used in this standards document.

ID	***Primary Attribute***	***Secondary Attribute***
1	Storage Subsystem Hardware (HW)	Workload
		Minimum IO/sec
		Minimum Throughput
		Storage unit uptime
		Universal Device ID value (UDID)
		Redundancy
		FC - Hosts to Storage Connectivity
		iSCSI - Hosts to Storage Connectivity
		FICON connectivity
		SCSI Initiator (Host Connections)
		Replication
		LUN creation
		LUN Expansion
		Storage provisioning
		Tiering capability
		Resource partitioning capability
		Dynamically tuning
		Backend Storage virtualization
		Snapshots
		Clones
		Storage device scale up capability
		Supported Disk type

		Return disk option
		Interoperability - Industry standards
		Firmware and microcode upgrade or updates
		Boot from SAN
		Operating system and file system compatibility
		Applications compatibility (minimum)
		Redundant Array of Independent Disk (RAID) levels
		RAID group size
		Power switches
		Standardized layouts
		Additional servers
		Role-based access
		Documentation
2	Mainframe support	Parallel Access Volume (PAV)
		FICON support
		HiperPAV support
		SMF support
		Emulation types
		Solid State devices (SSD) support on Mainframe
		Dynamic Channel Reconfiguration support
		MIDAW support
		Priority I/O Queuing
3	Storage Management Software	Enterprise license not based on capacity
		Interoperability
		Storage Reporting

		Automated tools for LUN provisioning
		Proactive monitoring and remote notification
		Single storage management console
		Additional servers
		Management server security
		Data snapshot (local)
		Performance analysis
		Storage Capacity planning
		Local copy
		Consistent design
4	Hardware/Software technical support	Support procedures
		Support Availability
		License transfer
		OEM resources
		Support Interface
		Disruptive patches
		SLAs
		Professional services
5	Hardware/software Installation	Installation
		Pre-configuration
		Onsite impact
		Necessary software/hardware
		Delivery
		Trash

		OS installation and security
6	Training	Training Length
		Knowledge transfer
		Documentation

B. Taxonomy of Tier2 and Tier3 Storage Standards, the followings are primary and secondary attributes used in this standards document.

ID	***Primary Attribute***	***Secondary Attribute***
1	Storage Subsystem Hardware (HW)	Workload
		Minimum IO/sec
		Minimum Throughput
		Storage unit uptime
		Universal Device ID value (UDID)
		Redundancy
		FC - Hosts to Storage Connectivity
		iSCSI - Hosts to Storage Connectivity
		SCSI Initiator (Host Connections)
		Replication
		LUN creation
		LUN Expansion
		Storage provisioning
		Tiering capability
		Deduplication
		Snapshots
		Clones
		Storage device scale up capability
		Supported Disk type

		Return disk option
		Interoperability - Industry standards
		Firmware and microcode upgrade or updates
		Boot from SAN
		Operating system and file system compatibility
		Applications compatibility (minimum)
		Redundant Array of Independent Disk (RAID) levels
		RAID group size
		Power switches
		Standardized layouts
		Additional servers
		Role-based access
		Documentation
2	Storage Management Software	Enterprise license not based on capacity
		Interoperability
		Storage Reporting
		Automated tools for LUN provisioning
		Proactive monitoring and remote notification
		Single storage management console
		Additional servers
		Management server security
		Data snapshot (local)
		Performance analysis

		Storage Capacity planning
		Local copy
		Consistent design
3	Hardware/Software technical support	Support procedures
		Support Availability
		License transfer
		OEM resources
		Support Interface
		Disruptive patches
		SLAs
		Professional services
4	Hardware/software Installation	Installation
		Pre-configuration
		Onsite impact
		Necessary software/hardware
		Delivery
		Trash
		OS installation and security
5	Training	Training Length
		Knowledge transfer
		Documentation

C. Taxonomy of STORAGE AREA NETWORK (SAN) Standards, the following is primary and secondary attributes used in this standards document.]

ID	***Primary Attribute***	***Secondary Attribute***
1	LAN Connectivity	IP Connectivity between Hosts and Storage device
2	Fabric switch hardware (HW)	Fabric Connectivity between Hosts and Storage device
		Interoperability
		Fabric Isolation
		Capacity “Throughput”
		Capacity “Ports”
		Port virtualization
		Manageability
		Fully redundant configuration
		Oversubscription
		Fabric
		Automated monitoring
		Current generation equipment
		Additional ports
		Rack Configuration
		Manageable power supplies
		Cooling
		Physical layout
		Standardized layouts
		Additional servers
		Role-based access
3	SAN Management Software	Management Software
		SAN Reporting

		Proactive monitoring and remote notification
		Performance monitoring
		Single SAN management console
		Additional servers
		Management server security
		Consistent design
4	Hardware/Software technical support	Support procedures
		Support Availability
		License transfer
		OEM resources
		Support Interface
		Disruptive patches
		SLAs
		Professional services
5	Hardware/software Installation	Installation
		Pre-configuration
		Onsite impact
		Necessary software/hardware
		Delivery
		Trash
		OS installation and security
		Single-initiator zoning
6	Training	Training Length
		Knowledge transfer

		Documentation

D. Taxonomy of General Backup and Archive standard, the followings are primary and secondary attributes used in this standards document.

ID	***Primary Attribute***	***Secondary Attribute***
1	Backup Method	Tape
		Disk (Tapeless)
		Archive
2	Virtual tape library (VTL) hardware	Technology
		Disk health monitoring
		Deduplication
		Replication
		Raw Storage Capacity
		Number of Emulated Tape Libraries
		Number of Emulated Tape Drives
		Number of Virtual Tape Cartridges
		Connectivity
		Redundancy
3	Archive Hardware	Technology
		Disk health monitoring
		Data Storage Architecture
		Deduplication
		Replication
		Protocol Support
		Number of Files
		File Size

		Raw Storage Capacity
		Number of drives
		Connectivity
		Redundancy
4	Tape Library hardware	Interoperability - Industry standards
		Compatibility
		Backup SAN
		Connectivity
		Fully redundant configuration
		Current generation equipment
		Library Capacity (throughput)
		Capacity (slots)
		Scalability (throughput)
		Scalability (slots)
		Rack Configuration
		Manageable power supplies
		Cooling
		Physical layout
		Size
		Standardized layouts
		Additional servers
		Online maintenance
5	Backup Software/VTL/Archive/ Tape library tool	Backup Software
		Tape Library management tool
		Encryption
		Compatibility

		Scripting
		Proactive monitoring and remote notification
		Role-based access
		Manageability
		Additional servers
		Management server security
		Consistent design
6	Hardware/Software technical support	Support procedures
		Support Availability
		License transfer
		OEM resources
		Support Interface
		Disruptive patches
		SLAs
		Professional services
7	Hardware/software Installation	Installation
		Pre-configuration
		Onsite impact
		Necessary software/hardware
		Delivery
		Trash
		OS installation and security
8	Training	Training Length
		Knowledge transfer
		Documentation

APPENDIX A – DEFINITIONS

APPENDIX B – REFERENCES

APPENDIX C – ACRONYMS

Refer to the VA Acronym Lookup Web page for a list of VA specific acronyms.

EIE VA OI&T Enterprise Infrastructure Engineering

Click here to enter additional acronyms.

APPENDIX D – CONTRIBUTORS

The following subject matter experts have contributed to the development of this document as indicated

Name	Organization	Role
Mark Zimmermann	VA	Identify VistA requirements
MSV contract team	HP	Identify VistA requirements
James Yaple	VA	Author
Paul Whiddon	VA	Author
Scott Price	VA	Author
Denise McLain	VA	Author
Mike Condon	VA	Author
John Kutzschebauch	VA	Author
Robert Moser	VA	Author
Carl Dahlstedt	VA	Author
John Hina	VA	Author
Evan Yeoh	VA	Author
Sue Drain	VA	Author

DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INFORMATION AND TECHNOLOGY

ENTERPRISE INFRASTRUCTURE ENGINEERING

VA Enterprise IT Infrastructure Standard

Data Center Standard

Revision 1.0

November 13, 2009

TABLE OF CONTENTS

1 Introduction 1

1.1 Purpose 1

1.2 Objectives 1

1.3 Scope 1

2 Standards 3

2.1 Support Infrastructure 3

2.2 Transport Media and Interfaces 5

2.3 Enclosure Power Distribution 7

2.4 Remote Management Technology 8

3 Supporting Details for Standards 10

3.1 Support Infrastructure 10

3.1.1 Equipment Enclosure 10

3.1.2 Open Rack 12

3.1.3 Cable Tray 13

3.1.4 Horizontal Cable Management Panels 14

3.1.5 Vertical Cable Management Panels 15

3.1.6 Fiber Distribution Cabinets 16

3.2 Transport Media and Interfaces 17

3.2.1 Patch Panels 17

3.2.2 Fiber Distribution Cassettes 18

3.2.3 UTP (Horizontal Distribution) 19

3.2.4 Fiber Optic Cable (Horizontal Distribution) 20

3.2.5 UTP Patch Cords 21

3.2.6 Fiber Patch Cords 21

3.3 Enclosure Power Distribution 22

3.3.1 Power Distribution Units (in rack/enclosure) 22

3.3.2 Zone Power Distribution Units 24

3.4 Remote Management Technology 25

3.4.1 KVM 25

4 Taxonomy of Standards 27

Appendix A – Definitions 32

Appendix B – References 32

Appendix C – Acronyms 33

Appendix D – Contributors 33

1 INTRODUCTION

1.1 PURPOSE

A standard is a set of rules or requirements that are determined by a consensus opinion of subject matter experts and prescribe criteria for a product, process, test or procedure. The general benefits of a standard are quality, interchangeability of parts or systems, and consistency. Information Technology (IT) standards are based on business needs provided through or supported by IT Services. IT Services are designed to support business processes and are constructed from software, hardware and infrastructure components. Establishing and enforcing standards for the selection and configuration of these supporting components improves the maintainability, reliability and availability of IT Services within projected economic constraints in alignment with business needs.

This standards document lists the acceptable and recommended specifications for Data Center passive Inside Plant, including racks, equipment enclosures, fiber and copper transport media, KVM, and rack-level power distribution. Sections include standard specifications for subject components, decisions supporting the standard specifications, guidelines or recommendations for implementing the standard specifications, and supplemental factors to consider when evaluating subject components. Other supplementary documents will provide guidance on procuring components that meet the standard specifications, guidance on integrating them with existing components, and explanation of how the subject components fit into the VA Architecture.

1.2 OBJECTIVES

This standard provides acceptable and recommended specifications to support:

- Solution Evaluation
- Requirement Evaluation
- Solution Design
- Solution Procurement and Bid Evaluation
- Evaluation of Architectural Specifications
- Standardization of passive Inside Plant infrastructure across all VA data centers

1.3 SCOPE

This standard applies to:

- Server Enclosures
- Open Racks
- Horizontal Cabling (Fiber)
- Horizontal Cabling (UTP)

- KVM
- Patch Panels
- Fiber Distribution Cabinets and Cassettes
- Patch Cords (UTP and Fiber)
- Cable Management
- In-Rack or Enclosure Power Distribution

2 STANDARDS

2.1 SUPPORT INFRASTRUCTURE

[Populate this table from the taxonomy in section 4 and enter specifications as necessary. Replace this paragraph with a brief description of this specification set.]

ID	***Primary Attribute***	***Secondary Attribute***	***Specification***
1	Equipment Enclosure	Dimensions	Height (nominal): 84” Width (overall): 24.0” Depth (w/ doors): 47.4”
		Rail Style	Square-punched (2 pair = front + rear) Tooless Adjustable
		Front Door	Single Perforated Reversible Swing
		Rear Door	Single Solid (heat containment). OR Split, perforated (no thermal management)
		Latches	Keyed lock upgradable to keyless system Compression Latch
		Color	White or Existing Match
		Top Panel	23.4” x 27.4” Vertical Exhaust Duct (heat containment) High Capacity Cable Access w/Brushes
		Side Panel	Solid (heat containment) Locking
		Baying Kit	Baying Kit
		Air Dam & Sealing Kit	Air Dam & Sealing Kit

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
		Castors	Castors (max 4.28” added height)
		Rack Units	45
		Green Technology	Heat containment per Data Center cooling architecture
		RU Marks	Present on front and rear rails
		Static Capacity	2,500 lbs
		Bonding Connection Points	Doors and frame
2	Open Rack	Dimensions	Height: 86” Width: 23.75” Depth: 26.2”
		Channel Depth	16.25”
		Rail Style	EIA, threaded, front/rear
		Rack units	45
		Static Capacity	1,500 lbs.
		Cable Management	Built in overhead “waterfall” and channel cable management strap attachment points
		RU Marks	Present on front and rear rails
3	Cable Tray	Design	Wire Basket
		Color	Black Powder Coated (ASTM B633)
		Capacity	Initial fill ratio not to exceed 60%
		Bonding Kit	Bonding Kit
		Toolless Splice Kits	Toolless spice kit to join segments
		Large Bend Radius Kits	One per bend
		Grounding Lug Kit	One per segment
4	Horizontal Cable Management Panels	Rack Units	2 RU (up to 100 Cat 6a patch cords) 1 RU (up to 50 Cat 6a patch cords)
		Finger Spacing	Six-port
		Cover	Double-hinged

ID	Primary Attribute	Secondary Attribute	Specification
		Capacity	50 Cat 6a or 100 Cat 6a
5	Vertical Cable Management Panels	Dimensions	16" x 13" x 7' (Ultra-high density) 12" x 13" x 7 (High density
		Door	Double-hinged
		Capacity	948 Category 6a patch cords 630 Category 6a patch cords
6	Fiber Distribution Cabinets	Cassette Capacity	3 Cassettes
		Rack Units	1 RU
		Access Door	Hinged front panel. No front door
		Internal Strand Mgmt	N/A

2.2 TRANSPORT MEDIA AND INTERFACES

[Populate this table from the taxonomy in section 4 and enter specifications as necessary. Replace this paragraph with a brief description of this specification set.]

ID	Primary Attribute	Secondary Attribute	Specification
1	Copper Patch Panels	Performance Category	Category 6a (10 GbE)
		Position Count	24 (4 six-port modules)
		Form Factor	Angled
		Size	One RU
		Color Coding	Black
2	Fiber Distribution Cassettes	Cassette Capacity	24 strand (two 12-strand MPOs). 50 micron.
		Cassette User Interfaces	LC quad connectors
		Cassette Backbone Interfaces	MPO

ID	*Primary Attribute*	*Secondary Attribute*	*Specification*
		Performance Characteristics	Laser Enhanced 10 GbE 50/125 Multimode
		Form Factor	1 U
3	UTP (Horizontal Dist.)	Performance Category	Category 6a (10 GbE)
		Performance Specifications	Meets or exceeds TIA-EIA-568-B.2-10, TSB-155.
		Smoke Rating	Plenum rated
		Jacket Color	Blue
		Termination Method	Pre-terminated, Bifurcated termination method
		Media Connector	Pre-terminated with split 8P8C
		Bundling	Multiple cable harness
4	Fiber (Horizontal Dist.)	Performance Category	Backbone Ribbon, Laser Enhanced to 10 GbE
		Performance Specifications	Laser Optimized 50/125 µm fibers with effective Modal Bandwidth equal or greater than 2000 MHz•km at 850 nm
		Mode	Multimode 50/125
		Smoke Rating	Plenum
		Jacket Color	Teal
		Termination Method	Pre-terminated / Factory terminated
		Media Connector	Pre-terminated with MPO
		Strand Count	12 per assembly
		Bundling	Loose Tube
5	UTP Patch Cords	Performance Category	Category 6a 26 gauge Stranded
		Performance Specifications	Center tuned to Horizontal media
		Jacket Color	Blue (per 606A)

ID	Primary Attribute	Secondary Attribute	Specification
		Termination Method	Factory pre-terminated
6	Fiber Patch Cords	Performance Category	Laser enhanced, 50/125 multimode
		Performance Specifications	10 Gb
		Jacket Color	Teal
		Termination Method	Factory pre-terminated

2.3 ENCLOSURE POWER DISTRIBUTION

[Populate this table from the taxonomy in section 4 and enter specifications as necessary. Replace this paragraph with a brief description of this specification set.]

ID	Primary Attribute	Secondary Attribute	Specification
1	Power Distribution Units (in rack/enclosure)	Receptacle Type(s)/Quantities	QTY three (3) C-19 QTY twenty-one (21) C-13
		Power Cord Plug	L21-20P
		kW Rating	Between 5 and 6 kW
		Volt Rating	208 Preferred 110 Available
		Management	Power Utilization Per Phase Monitor LED Display for Utilization SNMP v3 or SSH Supported for Remote Power Management and Monitoring Ethernet with IP Supported Serial Port Breakered Breaker must be protected from accidental shut-off Remote Power On/Off Per Outlet

ID	Primary Attribute	Secondary Attribute	Specification
			User Authentication (AD Integration Preferred) Threshold Alarms Intuitive and Consistent Outlet Naming Scheme
		Mounting	Zero RU Toolless
		Phase type	Three-phase
2	Zone Power Distribution Units	Rack Units	2
		Phase Type	3-phase WYE (four wire)
		Receptacle Type(s)/Quantities	QTY four (4) L21-20R QTY six (6) NEMA 5-15/20R
		Power Cord Plug	Dual L21-20P
		kW Rating	22-24 kW
		Volt Rating	208
		Fault Tolerance	Two inputs, 5 receptacles on each leg
		Mounting	Rack mount

2.4 REMOTE MANAGEMENT TECHNOLOGY

[Populate this table from the taxonomy in section 4 and enter specifications as necessary. Replace this paragraph with a brief description of this specification set.]

1	KVM Switch	Target Cable Requirements	UTP Support to 150 Feet (OOB)
		Server Interface Support	USB and PS2
		Authentication	Active Directory Integration
		Uplinks	Redundant

			1 GbE
		Encryption	SSL
		Logging	Activity Logging/Syslog
		Centralized Management	
		Local User	8 Local Users
		Remote User	
		Modem	
		Protocol Support	IP-based Access for Remote Users
		Client Software Support	Browser (MS Explorer and FireFox)
		Server Ports	64 interfaces for KVM
		Resolution	1600x1200
		Virtual Media Support	Virtual Media Support with Encryption
		Simultaneous Users	Up to 8 Simultaneous Users
		Management	SNMP Support

3 SUPPORTING DETAILS FOR STANDARDS

3.1 SUPPORT INFRASTRUCTURE

3.1.1 EQUIPMENT ENCLOSURE

STANDARD

ID	Secondary Attribute	Specification
1	Dimensions	Height: 83.5” Width: 23.6” Depth: 47.1”
	Rail Style	Square-punched (2 pair = front + rear)
	Front Door	Single Perforated
	Rear Door	Single Solid (heat containment) * OR Split, perforated (no thermal management)
	Latches	Keyed Lock. Cam Latch.
	Color	White
	Top Panel	23.4” x 27.4” Vertical Exhaust Duct* and High Capacity Cable Access
	Side Panel	Solid (heat containment)
	Baying Kit	Baying Kit
	Air Dam & Sealing Kit	Air Dam & Sealing Kit*
	Castors	Castors
	Rack Units	45
	Green Technology	Heat containment per Data Center cooling architecture*
	RU Marks	Present on front and rear rails
	Static Capacity	2,500 lbs See Implementation Guidance for seismic bracing.
	Bonding Connection Points	Doors and frame

EXPLANATION OF STANDARD

These specifications define a standardized server enclosure with sufficient depth to accommodate active hardware and cable management. The total depth will not exceed 48 inches or two floor tiles. The width will not exceed 24 inches or one floor tile. This standard specifies green technology in the form of heat containment. This approach to thermal management does have corresponding data center design requirements and, therefore, should be selected based on the cooling architecture of the target data center. If the facility cannot accommodate heat containment, the noted items (*) can be waived from this specification.

EVALUATION FACTORS

- Dimensions
- Vertical exhaust duct/heat containment
- Available Rack Units

IMPLEMENTATION GUIDANCE

Enclosures shall be equipped with seismic bracing when deployed in areas prone to earthquakes or as required by Federal regulation or other Authorities-Having-Jurisdiction (AHJ) and best practices

3.1.2 OPEN RACK

STANDARD

ID	Secondary Attribute	Specification
2	Dimensions	Height: 86” Width: 23.75” Depth: 26.2”
	Channel Depth	16.25”
	Rail Style	EIA hole pattern, threaded, front/rear
	Rack units	45
	Static Capacity	1,500 lbs.
	Cable Management	Built in overhead “waterfall” and channel cable management strap attachment points
	RU Marks	On front and rear rails

EXPLANATION OF STANDARD

This standard specifies a deep channel open rack to accommodate the depth and weight of most data networking equipment while providing high capacities for horizontal cable and large diameter Category 6a patch cords.

EVALUATION FACTORS

- Dimensions
- Cable management capacities
- Available accessories for horizontal and vertical cable management
- Static capacity

IMPLEMENTATION GUIDANCE

3.1.3 CABLE TRAY

STANDARD

ID	Secondary Attribute	Specification
3	Design	Wire Basket
	Color	Black Powder Coated (ASTM B633)
	Capacity	Initial fill ratio not to exceed 50%
	Bonding Kit	Bonding Kit
	Toolless Splice Kits	Toolless spice kit to join segments
	Large Bend Radius Kits	One per bend
	Grounding Lug Kit	One per segment

EXPLANATION OF STANDARD

This standard offers consistency in the construction characteristics of overhead cable tray to achieve common mounting, hanging, support, bonding, and interconnecting features for the benefit of data center designers and end-users.

EVALUATION FACTORS

- Wire-basket construction
- Tooless joining kits
- ASTM coating

IMPLEMENTATION GUIDANCE

3.1.4 HORIZONTAL CABLE MANAGEMENT PANELS

STANDARD

ID	Secondary Attribute	Specification
4	Rack Units	2 RU (up to 100 Cat 6a patch cords) 1 RU (up to 50 Cat 6a patch cords)
	Finger Spacing	Six-port
	Cover	Double-hinged
	Capacity	50 Cat 6a or 100 Cat 6a

EXPLANATION OF STANDARD

This standard creates uniform high-capacity horizontal cable management for Category 6a patch cords.

EVALUATION FACTORS

- Rack units
- Finger spacing
- Double-hinged cover
- Capacity

IMPLEMENTATION GUIDANCE

3.1.5 VERTICAL CABLE MANAGEMENT PANELS

STANDARD

ID	*Secondary Attribute*	*Specification*
5	Dimensions	16" x 13" x 7’ (Ultra-high density) 12" x 13" x 7 (High density)
	Door	Double-hinged
	Capacity	948 Category 6a patch cords 630 Category 6a patch cords

EXPLANATION OF STANDARD

This standard creates uniform high-capacity and ultra-high capacity vertical cable management for Category 6a patch cords.

EVALUATION FACTORS

- Dimensions
- Capacity

IMPLEMENTATION GUIDANCE

3.1.6 FIBER DISTRIBUTION CABINETS

STANDARD

ID	*Secondary Attribute*	*Specification*
6	Cassette Capacity	3 Cassettes
	Rack Units	1 RU
	Access Door	Hinged front panel. No front door
	Internal Strand Mgmt	N/A

EXPLANATION OF STANDARD

This standard specifies a small, modular enclosure for mounting MPO/SC fiber cassettes. The smallest form-factor has been selected for application flexibility.

EVALUATION FACTORS

- Form factor
- No front door
- 3 cassette capacity

IMPLEMENTATION GUIDANCE

Horizontal cabling, including fiber and UTP, should be installed in a structured topology with patch panels serving as Equipment Distributors (ED) and a corresponding set of patch panels located at a Horizontal Cross Connect (HC). The HC should be located adjacent to switching components to minimize patch cord length and cable management requirements. See Standards.

ED Fiber Distribution Cabinets will be installed in RU 45 of each enclosure where required.

3.2 TRANSPORT MEDIA AND INTERFACES

3.2.1 PATCH PANELS

STANDARD

ID	*Secondary Attribute*	*Specification*
1	Performance Category	Category 6a (10 GbE)
	Position Count	24 (4 six-port modules)
	Form Factor	Angled
	Size	One RU
	Color Coding	Black

EXPLANATION OF STANDARD

This standard anticipates the deployment of 10 gigabit Ethernet in production and test data centers. This standard can be applied to field-terminated 10 GbE or factory pre-terminated (preferred) applications.

EVALUATION FACTORS

- Performance category
- Form factor
- Compatibility with pre-terminated cable interfaces

IMPLEMENTATION GUIDANCE

Horizontal cabling, including fiber and UTP, should be installed in a structured topology with patch panels serving as Equipment Distributors (ED) and a corresponding set of patch panels located at a Horizontal Cross Connect (HC). The HC should be located adjacent to switching components to minimize patch cord length and cable management requirements. See Standards.

ED patch panels will be installed in the top five rack units of each enclosure (except SAN)

3.2.2 FIBER DISTRIBUTION CASSETTES

STANDARD

ID	*Secondary Attribute*	*Specification*
2	Cassette Capacity	24 strand (two 12-strand MPOs). 50 micron.
	Cassette User Interfaces	LC quad connectors
	Cassette Backbone Interfaces	MPO
	Performance Characteristics	Laser Enhanced 10 GbE 50/125 Multimode
	Form Factor	1 U

EXPLANATION OF STANDARD

This standard specifies one component of the structured cabling system for fiber optic cabling in the data center. It is the fiber equivalent to UTP patch panels. It requires 1- strand 10 GbE laser-enhanced ribbon backbone fiber cable (specified elsewhere in this document) pre-terminated with MPO connectors. Each cassette supports two 12-strand cable assemblies for a total capacity of 12 duplex SC interfaces. Three of these devices can be installed in the specified fiber distribution cabinet.

EVALUATION FACTORS

- Performance characteristics
- Form factor
- Interfaces

IMPLEMENTATION GUIDANCE

3.2.3 UTP (HORIZONTAL DISTRIBUTION)

STANDARD

ID	*Secondary Attribute*	*Specification*
3	Performance Category	Category 6a (10 GbE)
	Performance Specifications	Meets or exceeds TIA-EIA-568-B.2-10, TSB-155.
	Smoke Rating	Plenum rated
	Jacket Color	Blue
	Termination Method	Pre-terminated, Bifurcated termination method
	Media Connector	Pre-terminated with split 8P8C
	Bundling	Multiple cable harness

EXPLANATION OF STANDARD

This standard specifies pre-terminated Category 6a Unshielded Twisted Pair (UTP) for horizontal distribution in production and test data centers. Pre-terminated cables require that distances between termination points are known. However, this approach results in rapid installation of horizontal data center cabling without risks associated with field termination including wire fragments, impaired cabling performance due to installation techniques, faulty terminations, etc.

EVALUATION FACTORS

- Performance characteristics
- Compatibility with specified patch panels

IMPLEMENTATION GUIDANCE

Horizontal cabling, including fiber and UTP, should be installed in a structured topology with patch panels serving as Equipment Distributors (ED) and a corresponding set of patch panels located at a Horizontal Cross Connect (HC). The HC should be located adjacent to switching components to minimize patch cord length and cable management requirements. See Standards.

ED patch panels will be installed in the top five rack units of each enclosure (except SAN)

3.2.4 FIBER OPTIC CABLE (HORIZONTAL DISTRIBUTION)

STANDARD

ID	*Secondary Attribute*	*Specification*
4	Performance Category	Backbone Ribbon, Laser Enhanced to 10 GbE
	Performance Specifications	Laser Optimized 50/125 µm fibers with effective Modal Bandwidth equal or greater than 2000 MHz•km at 850 nm
	Mode	Multimode 50/125
	Smoke Rating	Plenum rated
	Jacket Color	Teal
	Termination Method	Pre-terminated / Factory terminated
	Media Connector	Pre-terminated with MPO
	Strand Count	12 per assembly
	Bundling	Loose Tube

EXPLANATION OF STANDARD

This standard specifies laser-enhanced 50/125 multimode fiber-optic cable to be used in production and test data centers. Pre-termination requires that distances between termination points is known, however it assures maximum performance and rapid installation.

EVALUATION FACTORS

- Performance characteristics
- Pre-terminated with MPO connectors
- 12 strand, plenum rated, loose tube ribbon

IMPLEMENTATION GUIDANCE

Horizontal cabling, including fiber and UTP, should be installed in a structured topology with patch panels serving as Equipment Distributors (ED) and a corresponding set of patch panels located at a Horizontal Cross Connect (HC). The HC should be located adjacent to switching components to minimize patch cord length and cable management requirements. See Standards.

3.2.5 UTP PATCH CORDS

STANDARD

ID	Secondary Attribute	Specification
5	Performance Category	Category 6a 26 gauge Stranded
	Performance Specifications	Center tuned to Horizontal media connectors
	Jacket Color	Blue (per 606A)
	Termination Method	Factory pre-terminated

EXPLANATION OF STANDARD

This standard specifies center-tuned Category 6a patch cords. Inside Plant Design best practices dictate that component level compliance to a performance standard must be maintained across the entire horizontal link. The quality of patch cords and adherence to performance standards is critical to the reliable operation of a high-speed LAN.

Jacket color should be determined by ANSI/TIA/EIA 606A or other Inside Plant standard. Color coding the jacket to function may result in inventory management issues.

EVALUATION FACTORS

- Performance characteristics
- Center-tuned to installed patch panels

IMPLEMENTATION GUIDANCE

3.2.6 FIBER PATCH CORDS

STANDARD

ID	Secondary Attribute	Specification

6	Performance Category	10 Gigabit
	Performance Specifications	Laser enhanced, 50/125 multimode fiber, Duplex SC
	Jacket Color	Teal
	Termination Method	Factory pre-terminated

EXPLANATION OF STANDARD

This standard specifies high-bandwidth fiber patch cords. Inside Plant Design best practices dictate that component level compliance to a performance standard must be maintained across the entire horizontal link. The quality of patch cords and adherence to performance standards is critical to the reliable operation of a high-speed LAN or SAN.

EVALUATION FACTORS

- Performance characteristics
- Performance specifications

IMPLEMENTATION GUIDANCE

3.3 ENCLOSURE POWER DISTRIBUTION

3.3.1 POWER DISTRIBUTION UNITS (IN RACK/ENCLOSURE)

STANDARD

ID	*Secondary Attribute*	*Specification*
1	Receptacle Type(s)/Quantities	QTY three (3) C-19 QTY twenty-one (21) C-13
	Power Cord Plug	L21-20P
	kW Rating	Between 5 and 6 kW
	Volt Rating	208

	Management	Power Utilization Per Phase Monitor LED Display for Utilization SNMP v3 or SSH Supported for Remote Power Management and Monitoring Ethernet with IP Supported Serial Port Breakered Breaker must be protected from accidental shut-off Remote Power On/Off Per Outlet User Authentication (AD Integration Preferred) Threshold Alarms Intuitive and Consistent Outlet Naming Scheme
	Mounting	Zero RU, Toolless
	Phase type	Three-phase

EXPLANATION OF STANDARD

This standard creates uniform in-rack power distribution at 208 volt with IEC power outlets. This standard supports remote monitoring capability to provide real-time power consumption monitoring at the rack level. Power redundancy is supported by this standard by installing up to four PDUs per enclosure and splitting the power inputs across two circuits within the zone PDU.

EVALUATION FACTORS

- Outlet type and quantity
- Phase type
- kW rating
- Cord plug specification
- Remote monitoring

IMPLEMENTATION GUIDANCE

3.3.2 ZONE POWER DISTRIBUTION UNITS

STANDARD

ID	Secondary Attribute	Specification
2	Rack Units	2
	Phase Type	3-phase WYE (four wire)
	Receptacle Type(s)/Quantities	QTY four (4) L21-20R QTY six (6) NEMA 5-15/20R
	Power Cord Plug	QTY two (2) L21-30P
	kW Rating	22-24 kW
	Volt Rating	208
	Fault Tolerance	Two inputs, 5 receptacles on each leg
	Mounting	Rack mount

EXPLANATION OF STANDARD

This standard creates uniform zone power distribution at three-phase 208 volt with 110 step down if necessary. This standard supports power redundancy is supported by energizing up to four PDUs across two 30 amp, three-phase power feeds.

EVALUATION FACTORS

- Rack units
- Phase type
- 208 and 110 volt
- Dual inputs
- kW rating

IMPLEMENTATION GUIDANCE

3.4 REMOTE MANAGEMENT TECHNOLOGY

3.4.1 KVM

STANDARD

ID	*Secondary Attribute*	*Specification*
1	Target Cable Requirements	UTP Support to 150 Feet (OOB)
	Server Interface Support	USB and PS2
	Authentication	Active Directory Integration
	Uplinks	Redundant 1 GbE
	Encryption	SSL
	Logging	Activity Logging/Syslog
	Centralized Management	
	Local User	8 Local Users
	Remote User	
	Modem	
	Protocol Support	IP-based Access for Remote Users
	Client Software Support	Browser (MS Explorer and FireFox)
	Server Ports	64 interfaces for KVM
	Resolution	1600x1200
	Virtual Media Support	Virtual Media Support with Encryption
	Simultaneous Users	Up to 8 Simultaneous Users

EXPLANATION OF STANDARD

This standard creates uniform digital KVM over IP solution for remote access to USB and PS2 server interfaces. This standard supports secure remote access.

EVALUATION FACTORS

- -

IMPLEMENTATION GUIDANCE

4 TAXONOMY OF STANDARDS

[Build taxonomy of this standard, defining the primary and secondary attributes common to all standards sets that will be contained in this standard. Add additional rows and cells as necessary. This attribute set will be used to populate the tables in Sections 2 and 3. Replace this paragraph with a paragraph introducing your taxonomy.]

ID	***Primary Attribute***	***Secondary Attribute***
1	Enclosure	Dimensions
		Rail Style
		Front Door
		Rear Door
		Latches
		Color
		Top Panel
		Side Panel
		Baying Kit
		Air Dam & Sealing Kit
		Castors
		Rack Units
		Green Technology
		RU Marks
		Static Capacity
		Bonding Connection Points
2	Open Rack	Dimensions
		Channel Depth
		Rail Style
		Rack units

		Static Capacity
		Cable Management
		RU Marks
3	Cable Tray	Design
		Color
		Capacity
		Bonding Kit
		Toolless Splice Kit
		Large Bend Radius Kit
		Grounding Lug Kit
4	Horizontal Cable Management Panels	Rack Units
		Finger Spacing
		Cover
		Capacity
5	Vertical Cable Management Panels	Dimensions
		Door
		Capacity
6	Copper Patch Panels	Performance Category
		Position Count
		Form Factor
		Color Coding
7	Fiber Distribution Cabinets (Horizontal SAN & Data)	Cassette Capacity
		Rack Units
		Access Door
		Internal Strand Management

8	Fiber Distribution Cassettes	Cassette Capacity
		Cassette User Interfaces
		Cassette Backbone Interfaces
		Performance Characteristics
		Form Factor
9	UTP (Horizontal Distribution)	Performance Category
		Performance Specifications
		Smoke Rating
		Jacket Color
		Termination Method
		Media Connector
		Bundling
10	UTP Patch Cords	Performance Category
		Performance Specifications
		Jacket Color
		Termination Method
11	Fiber Patch Cords	Performance Category
		Performance Specifications
		Jacket Color
		Termination Method
12	Fiber Optic Cable (Horizontal Distribution)	Performance Category
		Performance Specifications
		Mode
		Smoke Rating
		Jacket Color

		Termination Method
		Media Connector
		Strand Count
		Bundling
13	Power Distribution Units (in rack/enclosure)	Receptacle Type(s)/Quantities
		Power Cord Plug
		kW Rating
		Volt Rating
		Monitoring
		Mounting
		Rack Units
		Phase Type
14	Zone Power Distribution Units	Receptacle Type(s)/Quantities
		Power Cord Plug
		kW Rating
		Volt Rating
		Fault Tolerance
		Mounting
		Rack Units
		Phase Type
15	KVM Switch	Target Cable Requirements
		Server Interface Support
		Authentication
		Uplinks
		Encryption

		Logging
		Centralized Management
		Local User
		Remote User
		Modem
		Protocol Support
		Client Software Support
		Server Ports
		Resolution
		Virtual Media Support
		Simultaneous Users

APPENDIX A – DEFINITIONS

Click here to enter definitions.

APPENDIX B – REFERENCES

ANSI/TIA/EIA-568-B.1
Commercial Building Telecommunications Cabling Standard.
Part 1: General Requirements 2001

ANSI/TIA/EIA-568-B.1.1
Commercial Building Telecommunications Cabling Standard.
Part 1. Addendum 2001

ANSI/TIA/EIA-568-B.2
Commercial Building Telecommunications Cabling Standard.
Part 2: Balanced Twisted Pair Components 2001

ANSI/TIA/EIA-568-B.3
Optic Fiber Cabling Components Standard 2000

ANSI/TIA/EIA-569-A
Addendums 1 through 6
Commercial Standard for Telecommunications Pathways and Spaces 1998

ANSI/TIA/EIA-606-A
Administration Standard for Commercial Telecommunications Infrastructure 2002

ANSI/TIA/EIA-J-STD-607-A
Commercial Building Grounding and Bonding Requirements for Telecommunications 2002

CSI MASTERFORMAT ™ 2004 EDITION NUMBERS & TITLES Construction Specifications Institute (CSI)

NECA/BICSI 568-2006Standard for Installing Commercial Building Telecommunications Cabling (ANSI) 2006

NFPA National Electric Code Handbook 2002

Telecommunication Distribution Methods Manual BICSI, Eleventh Edition 2006

VA DIRECTIVE 6500 INFORMATION SECURITY PROGRAM 2006

Federal Information Processing Standard (FIPS) 200Minimum Security Requirements for Federal Information and Information Systems2006

APPENDIX C – ACRONYMS

Refer to the VA Acronym Lookup Web page for a list of VA specific acronyms.

EIE VA OI&T Enterprise Infrastructure Engineering

Click here to enter additional acronyms.

APPENDIX D – CONTRIBUTORS

The following subject matter experts have contributed to the development of this document as indicated

Name	Organization	Role
Click here to enter list of subject matter experts and briefly describe their contribution to this document.		