



## Interagency Program Office Program Management Support

*IPO iEHR Volume 3 SOI Governance 10312013*



---

### IPO PM Support

Department of Defense / Department of Veterans Affairs Interagency Program Office

Document Number: Volume 3: Service Oriented Infrastructure (SOI)  
Release/Revision Status: Version 1.3  
Release/Revision Date: October 31, 2013  
File Name: IPO\_iEHR\_Volume\_3\_SOI\_Governance\_10312013.doc

**Unclassified**

---

This page left intentionally blank

## Approved By:

---

<Name>  
<Title>, <Organization>

---

Date

## Record of Changes

Date	Authors	Version	Change Reference
03/01/2013	Som Krishnamurthy Raju Prasannappa Joseph P Diliberto III	1.0	Initial Draft
05/15/2013	Raju Prasannappa	1.1	Updates
06/06/2013	Raju Prasannappa	1.2	Removed signature reference
09/03/2013	Raju Prasannappa	1.3	Formatting updated to follow IPO guidelines Updated diagrams

## Table of Contents

1-1. Introduction .....	1
1-2. Purpose.....	2
1-3. Scope.....	3
1-4. Target Audience.....	4
1-5. SOA Suite Environment .....	5
1-5.1 SOA Suite Description.....	5
1-5.2 SOA Suite Environment.....	5
1-5.2.1 System Capabilities.....	5
1-5.2.2 Software Environment.....	6
1-5.3 SOA Enterprise Service Bus Logical Hardware/Network Architecture .....	7
1-5.3.1 Hardware Environment .....	8
1-5.3.1.1 Architecture - Regional.....	8
1-5.3.1.2 Architecture - Local .....	8
1-5.3.2 Site Components .....	9
1-5.3.3 Naming Conventions.....	10
1-5.3.3.1 Machine Names .....	10
1-5.3.4 Domain Names .....	11
1-5.3.5 Internet Protocol Addresses.....	11
1-5.4 Security .....	11
1-5.5 External Interfaces.....	12
1-5.6 Network Topology.....	12
1-5.6.1 Interim (Network Solution).....	13
1-5.6.2 End State (Network Solution).....	13
1-5.7 Sandbox .....	17
1-5.7.1 Contractor Sandbox Located at the Harris Melbourne Facility .....	17
1-5.7.2 Government Sandbox located at the JITC ITEC Maui, Hawaii Facility .....	19
1-5.7.3 Sandbox Access .....	21
1-5.7.3.1 Access Methods.....	21
1-5.8 Development and Test Environment (DTE).....	23
1-5.9 Quality Assurance Environment (Staging).....	24
1-5.10 Pre-production Environment.....	24
1-5.11 Production .....	24
1-5.12 Failover and Load Balancing .....	24
1-5.13 Disaster Recovery and Backup .....	24
1-6. SOI Role in the Service Life Cycle .....	25
1-7. Developer On-boarding Process (SOI Infrastructure) .....	26
1-8. Service On-Ramping/Off-Ramping Process .....	27
1-8.1 Service On-Ramping Process .....	27

- 1-8.2 Service Off-Ramping Process ..... 29
- 1-9. Customer Support ..... 31
  - 1-9.1 Sandbox Support..... 31
  - 1-9.2 General SOA Suite Support ..... 31
  - 1-9.3 Education and Training..... 31
- 1-10. Configuration/Change Management ..... 32
  - 1-10.1 Change Requests..... 32
- 1-11. Appendix A – Acronyms ..... 33
- 1-12. Appendix B – SOA Suite Component Descriptions ..... 35
- 1-13. Appendix C – Error Message References ..... 37
  - 1-13.1 Background ..... 37
  - 1-13.2 Custom Error Messages..... 37
  - 1-13.3 COTS Error Message – References..... 38
- 1-14. References..... 40

## 1-1. Introduction

The Department of Defense (DoD)/Department of Veterans Affairs (VA) Interagency Electronic Health Record (iEHR) initiative is in the process of making Service Oriented Architecture (SOA) its primary architectural paradigm. Throughout this document “iEHR” will be used to represent the current initiative.

This document is the third in a series of documents that the iEHR Service Oriented Enterprise (SOE) Center of Excellence (CoE) is publishing to educate and guide stakeholders in adopting the SOA Suite infrastructure and comply with the standards being established by the CoE. The three documents being published are based on three key components needed for any organization to successfully adopt the SOA paradigm. The three key components are:

- **Service-Oriented Enterprise (SOE)** - The SOE implies a consistent, enterprise-wide approach to service orientation, including necessary organizational structures, and enterprise roadmap. Volume 1 describes the SOE including the SOA CoE.
- **Service-Oriented Architecture (SOA)** - The SOA implies an implementation of the SOA paradigm to include policies and practices for the governance of services. Volume 2 covers issues, policies and procedures related to SOA Governance.
- **Service-Oriented Infrastructure (SOI)** - The SOI consists of the hardware, network, virtualized servers, and operating systems necessary to enable the SOA. SOI is the foundational layer on which the SOA is implemented. This document, Volume 3, addresses all aspects of the infrastructure.

This document should be considered a living document and is subject to modification and refinement based on input from stakeholders as they start using the SOA Suite.

## **1-2. Purpose**

The purpose of this document is to establish a set of processes and policies, as well as provide overall guidance regarding the implementation and use of the SOI.

## **1-3. Scope**

This volume focuses on the SOI and provides an overview of the infrastructure and its governance including guidance for using the infrastructure by the providers and consumers of service and the role played by SOI in each phase of the service lifecycle.

Specifically, this document discusses the following topics:

- SOA infrastructure lifecycle
- Services infrastructure standards and policies
- Deployment management standards and policies
- Configuration/change management standards and policies
- Developer on-boarding standards, policies and processes
- Service on-ramping and off-ramping processes

A comprehensive risk management plan is in place as described in the Task Order Management Plan – SID 002 that addresses the SOA Suite components. The SOA governance will follow that plan described in that document.

## **1-4. Target Audience**

The intended audience of this volume are the divisions within the Office of the Chief Information Officer (OCIO), TRICARE Management Activity (TMA), the Interagency Program Office (IPO), the DoD Office of the Chief Technology Officer (OCTO), the Service Military Medical departments, the VA Office of Information Technology (OIT) Architecture Strategy and Design (ASD) and VA Service Delivery and Engineering (SDE), system administrators, system integrators, service management, monitoring teams, and other iEHR stakeholders, as appropriate. This document is intended to be refined in a collaborative manner with input from all stakeholders.

## 1-5. SOA Suite Environment

### 1-5.1 SOA Suite Description

From a functional perspective, the target end state (at high level) is shown in Figure 1. This diagram shows the joint functionality used by both the Military Health System (MHS) and VA as well as functionality unique to each organization. Figure 1 shows the target end state that uses a common graphical user interface (GUI), a set of commercial-off-the-shelf (COTS) modules, a SOA infrastructure, and a Common Information Interoperability Framework (CIIF) to support syntactic and semantic data exchange.

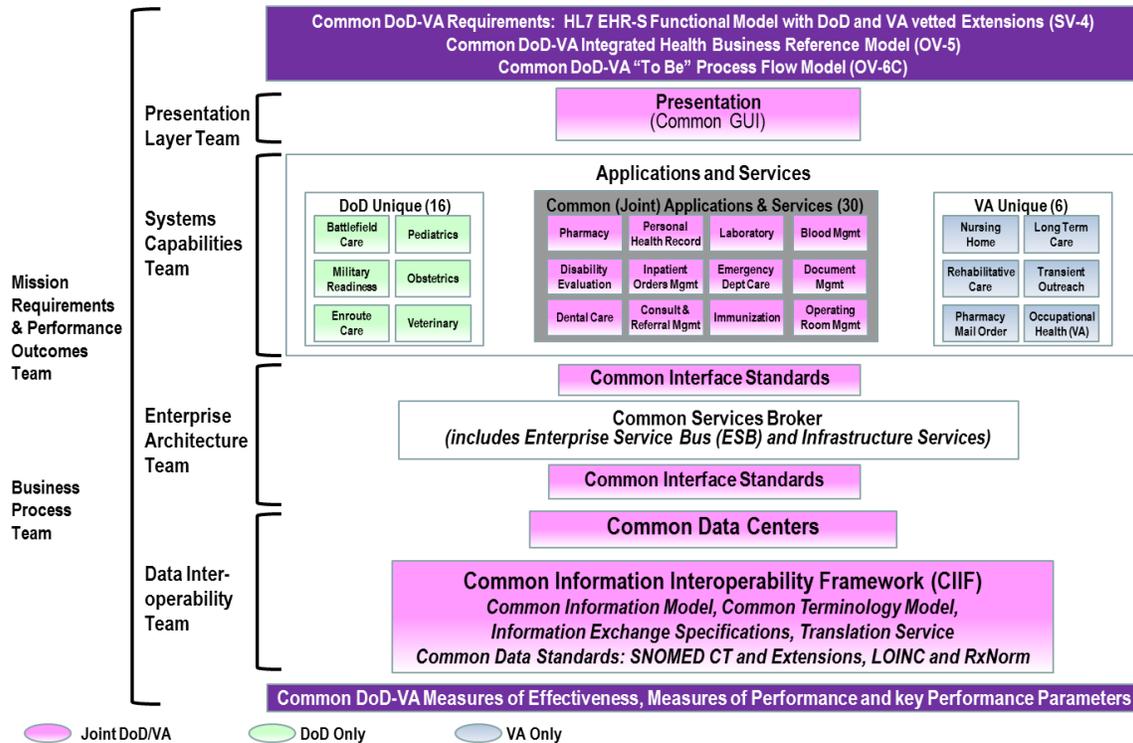


Figure 1 – High Level Representation of Functional and Infrastructure Components

The computing infrastructure of DoD MHS and VA must also evolve to provide capabilities that will be needed by the SOA Suite program. The core infrastructure services of the SOA Suite must be capable of quickly responding to the voluminous requests that will be levied upon them by users and mission applications of the iEHR community. DoD MHS and VA will also provide hardware, software, and facilities that will be used to host clinical health and business applications, databases, and storage to support users of the iEHR community. The provisioning of the equipment and facilities needed to support these capabilities must be synchronized with the anticipated demand, particularly with respect to the centrally hosted cloud, regional data centers and the local sites that will host services and/or store data.

## 1-5.2 SOA Suite Environment

### 1-5.2.1 System Capabilities

DoD and VA conducted analysis and concluded that a COTS SOA Suite-Enterprise Service Bus (ESB) with supporting services and sustainment will provide the necessary capability to manage the critical ESB functionality of the iEHR architecture. The purpose of the SOA Suite-ESB is to facilitate the data sharing

and application communication for the implementation of iEHR and provide the base capability from which the departments can proceed to leverage the capability to support broader exchange of information.

The architecture presented here promotes continuity of operations throughout the VA and MHS regionalization and consolidation processes in order to maximize performance.

The software architecture is built upon a highly-capable full-featured SOA Suite-ESB set at the federated enterprise level across a global set of regions that the Government has or will select as well as a lighter weight ESB capability at the local medical sites which maintain computing infrastructure for mission sustainment and for garrison and theater echelons of care where ESB capabilities are deemed appropriate and necessary. This approach manages complexity and cost against capability.

## 1-5.2.2 Software Environment

Table 1 lists all the software components of the SOA Suite and their current versions. The table also lists a brief description of the functionality of the software. An architectural overview of the various components is shown in Figure 10.

**Table 1 – Components of the SOA Suite by vendor**

COTS Component	Description	Version Number – Sept 15 release
IBM WebSphere Message Broker (WMB) v8.0.2	Core ESB messaging engine. Provides reliable messaging, queuing, and application workflow control.	8.0.0.2
IBM Business Process Server/ Business Manager (WPS/WBM) v7.5	Advanced Business Process Management services including BPEL capabilities, application choreography, and human task management / workflow	8.0.1.1
IBM WebSphere Service Registry and Repository (WSRR) v8.0	WSRR is used for SOA Governance; stores and manages design-time service definitions as well as functions as a run-time governance tool utilized by integration workflows to determine appropriate service endpoints to route to, based on SLAs and availability. It is also a Policy Decision Point (PDP) with regard to security policy management.	8.0.0.2
WebSphere Operational Decision Management (WODM) v8.0	WODM provides business rule management - a way to extract business logic from custom software / code and allow analysts to alter logic to suit new requirements without involving developers / recompiling code. Can be utilized within workflows (called by other SOA Suite components) or also as a foundational component for future application and service development. It is especially useful for business logic that is subject to frequent change (clinical decision support, regulatory management, etc.).	8.0.1.1
WebSphere Application Server (WAS) v8.0	Provides a Java application server "JEE container" for other services to be built for use with the SOA Suite / iEHR.	8.0.0.6
IBM DB2 v9.7	DB2 is a relational database management system provided by IBM to support various other IBM SOA Suite components like WSRR and WODM. It is not provided for other database use - only to support the SOA Suite products.	9.7.8
Layer 7 SecureSpan Gateway v7.1	The Layer 7 role includes a lightweight ESB including routing, orchestration, protocol translation, eXtensible Access Control Markup Language (XACML), federation, and Security Assertion Markup Language (SAML). The SecureSpan Gateway provides a means for consistent enforcement of policy in a distributed SOA at a granular XML or SOAP message level. The Gateway provides Transport Layer Security (TLS) and certificate management.	7.1

COTS Component	Description	Version Number – Sept 15 release
WebSphere Transformation Extenders v8.4	Data conversion services for SAP, Siebel, etc.	8.4.1
WebSphere Healthcare Connectivity Pack v8	Provides health connectivity such as HL7 MLLP.	8
CA Application Performance Management (APM)	Provides prescriptive insight into the infrastructure components needed to optimize IT operations. Supports ongoing planning and includes capabilities to plan new enterprise application deployments and changes in a virtualized environment.	9.1.7

For detailed descriptions of each SOA Suite component in the table above, please refer to



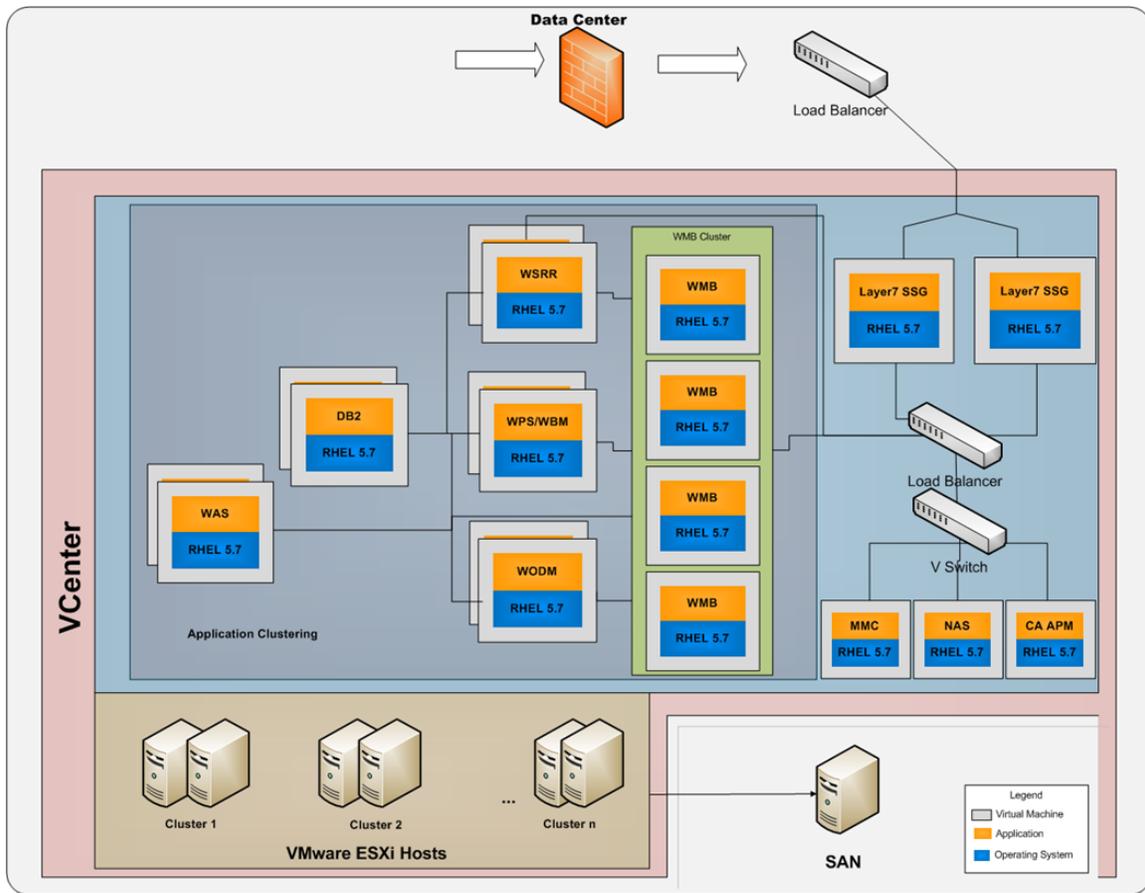


Figure 3 – High Level Regional Site Architecture

### 1-5.3.1.2 Architecture - Local

**Error! Reference source not found.** shows the local site architecture. It identifies the hardware topology, software running on each of the VM's, the firewall, load balancers and the SAN storage. This picture also shows the interaction between Mirth and Health Level Seven (HL 7) which provides the handshake between regional SOA suites and the local sites.

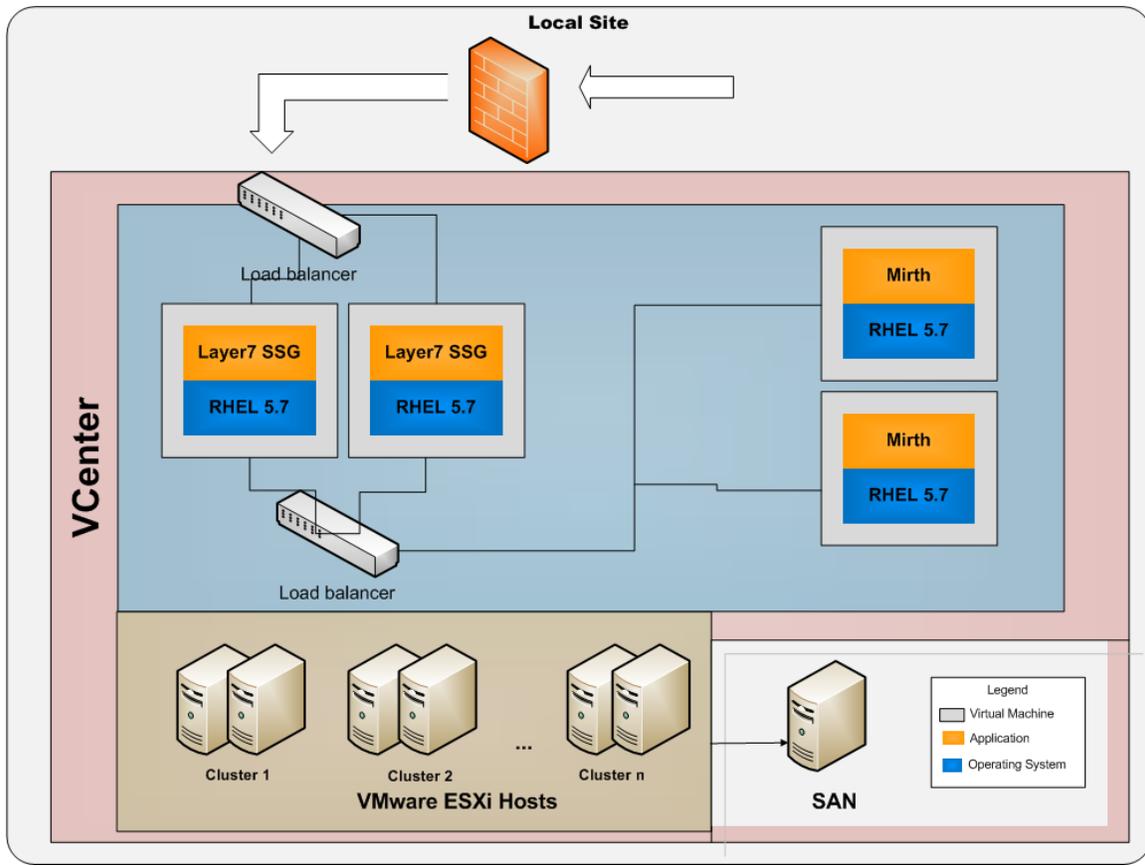
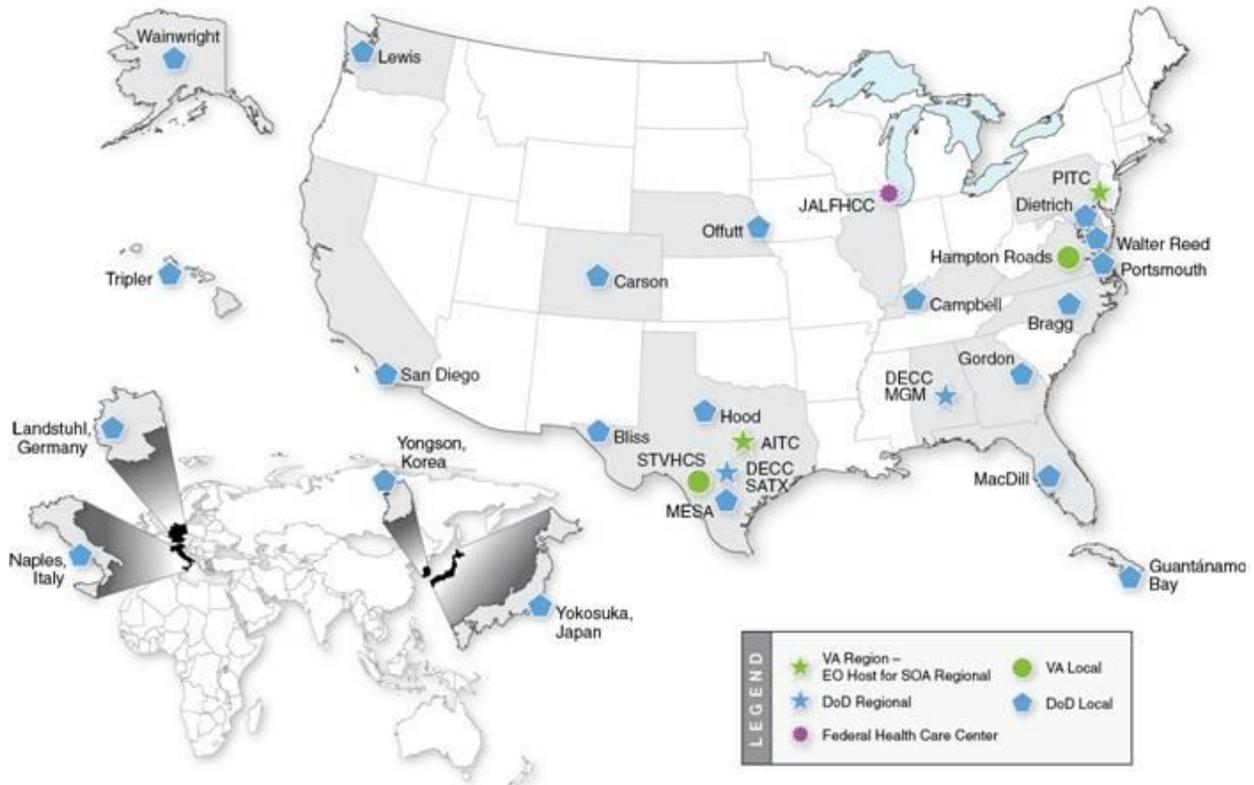


Figure 4 – High Level Local Site Architecture

### 1-5.3.2 Site Components

Deployment of the SOA Suite capabilities across both DoD and VA information infrastructure environments include the deployment sites shown in Figure 5.



Last updated: 08/12/2013

\*In calendar years.

Error! Reference source not found. Figure 5 – SOA Suite Sites - Overview with Schedule

### 1-5.3.3 Naming Conventions

#### 1-5.3.3.1 Machine Names

Hostnames in both regional and local sites are derived from a systematic approach generated using the algorithm below and defined in the Operations and Maintenance Plan – SID 045.

(Site ID) (Environment ID) (Application ID)(Instance Number - ## format)

The values for these parameters are listed in **Error! Reference source not found.** An example of a machine name derived from this could be: SOA-SITE\_001\_D\_SSG\_01 = DISA DECC Montgomery, Development, Layer 7 SecureSpan Gateway, 01 server.

Table 2 – Machine Name Parameters

Site IDs	Location
SOA-SITE_001	DISA DECC, Montgomery, AL
SOA-SITE_002	DISA DECC, San Antonio, TX
SOA-SITE_003	MESA
SOA-SITE_004	Audie L. Murphy Veterans Hospital

SOA-SITE_005	Hampton Roads VAMC
SOA-SITE_006	NMCP
Environment IDs	Description
D	Development
I	Integration
S	Staging
T	Testing
O	Operational
Application IDs	Description
APM	CA APM application monitor
DB2	IBM DB2 database server
MCT	Mirth Connect
ODM	IBM ILOG JRules WS Operational Decision Management (WODM)
SSG	Layer 7 Secure Span Gateway
WAS	IBM WebSphere Application Server
WMB	IBM WebSphere Message Broker
WPS	IBM WebSphere Process Server
WSR	IBM WebSphere Service Registry and Repository

If a need arises for a change in the naming convention of the machine name to one other than the defined above, a prior approval needs to be taken and approved by TWG/CoE team.

### 1-5.3.4 Domain Names

All domain names will use the .mil hierarchy owned by DISA. The domain name will be .csd.disa.mil. Addresses within .mil are available to .mil, .gov, and .com domains with proper accesses.

### 1-5.3.5 Internet Protocol Addresses

Internet Protocol (IP) addresses (IPv4/IPv6) are to be provided by DISA. If a requirement arises for a specific IP address, that needs to be raised as a special request to DISA with a justifiable business case of the need for a specific IP address.

## 1-5.4 Security

In support of system operations, which will provide services to DoD and VA healthcare providers, as well as, potentially, other organizations, the SOA Suite will have to support the long-term intent of the iEHR and must meet the security and privacy requirements of both DoD and VA. The document Security Management Plan – SID 046 describes in detail the ability of the SOA Suite system design to meet applicable information assurance (IA) requirements and the accreditation criteria. It satisfies the following Department of Defense Instruction (DoDI) 8500.2 IA controls, including a listing of applicable Federal Information Security Management Act (FISMA) requirements. This document describes the technical, administrative, and procedural IA program and policies that govern the SOA Suite-ESB and identifies all specific IA requirements and objectives such as, requirements for data handling or dissemination, system redundancy and backup or emergency response.

This references the security safeguards associated with external system interfaces and/or remote access solutions that are considered an integral part of the SOA Suite. For further details on the security process and policies refer to Security Management Plan – SID 046.

### 1-5.5 External Interfaces

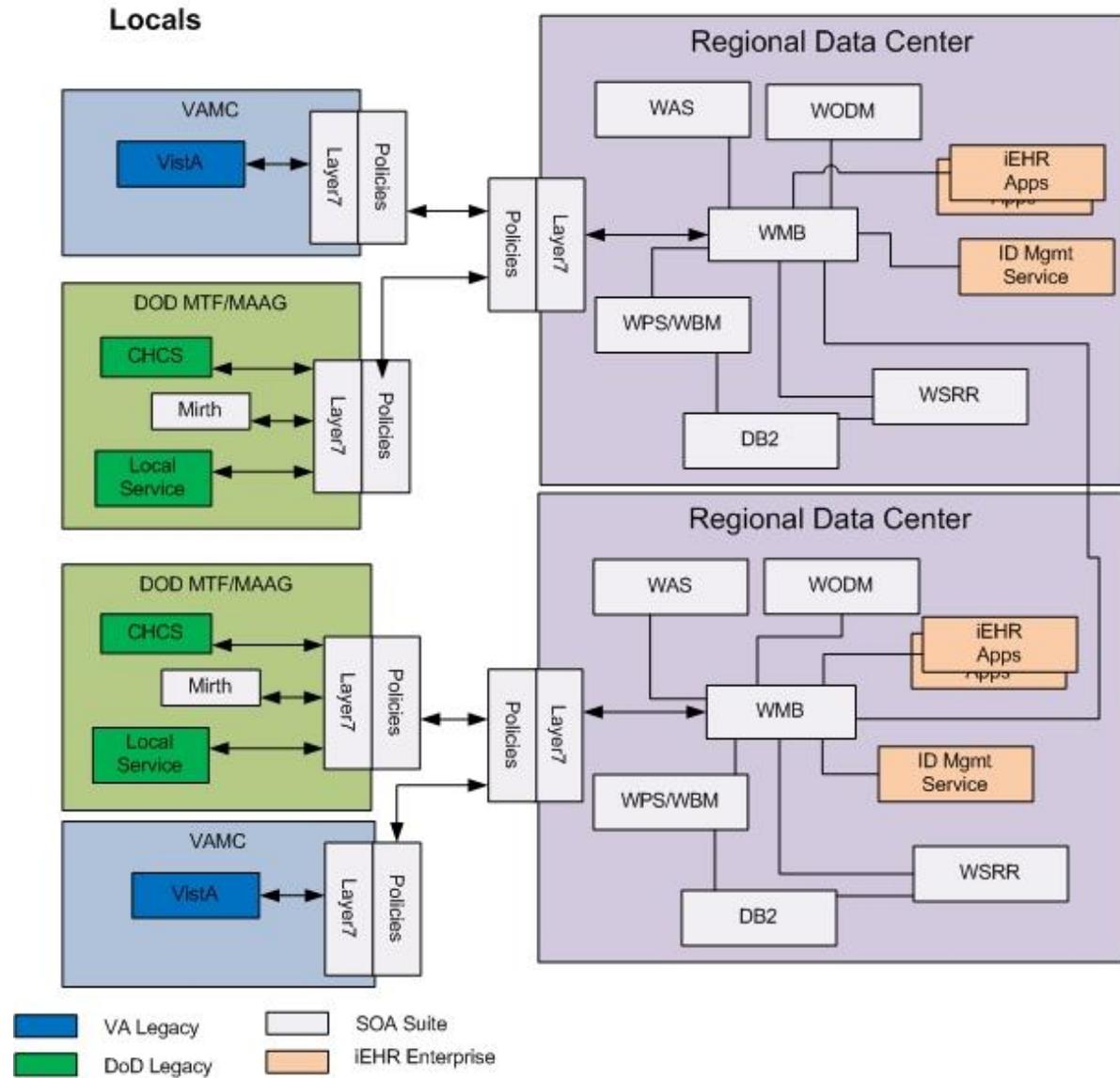


Figure 6 identifies all the external interfaces interacting with the SOA Suite, and also shows the handshake between local and regional sites.

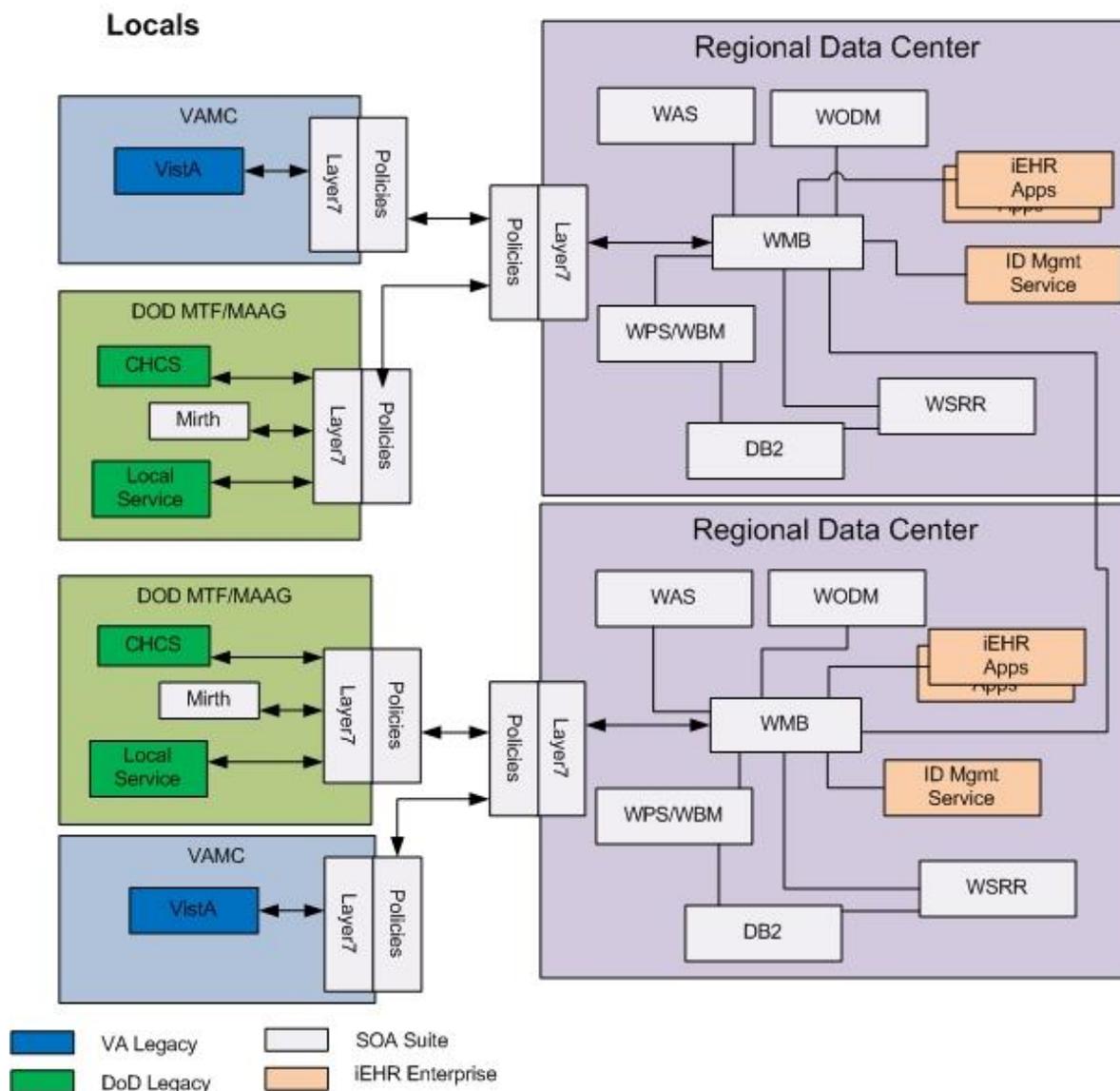


Figure 6 – External System Interfaces

## 1-5.6 Network Topology

The SOA Suite relies on the availability of a stable and efficient communication infrastructure, such as is being planned through the Medical Community of Interest (Med-COI). However, while that infrastructure is being put in place, the SOA Suite will leverage existing DoD/VA gateways for communication between and DoD and VA to provide an interim solution.

### 1-5.6.1 Interim (Network Solution)

Prior to the availability of Med-COI, the SOA Suite will be using an interim solution for communication between DoD and VA. Military Health System Intranet (MHSi) will be used for communications between the DoD sites and DISA Defense Enterprise Computing Center (DECC) and DoD/VA Gateway will be

used for VA site connectivity to DISA DECC. Figure 7 provides a simple representation of this interim solution.

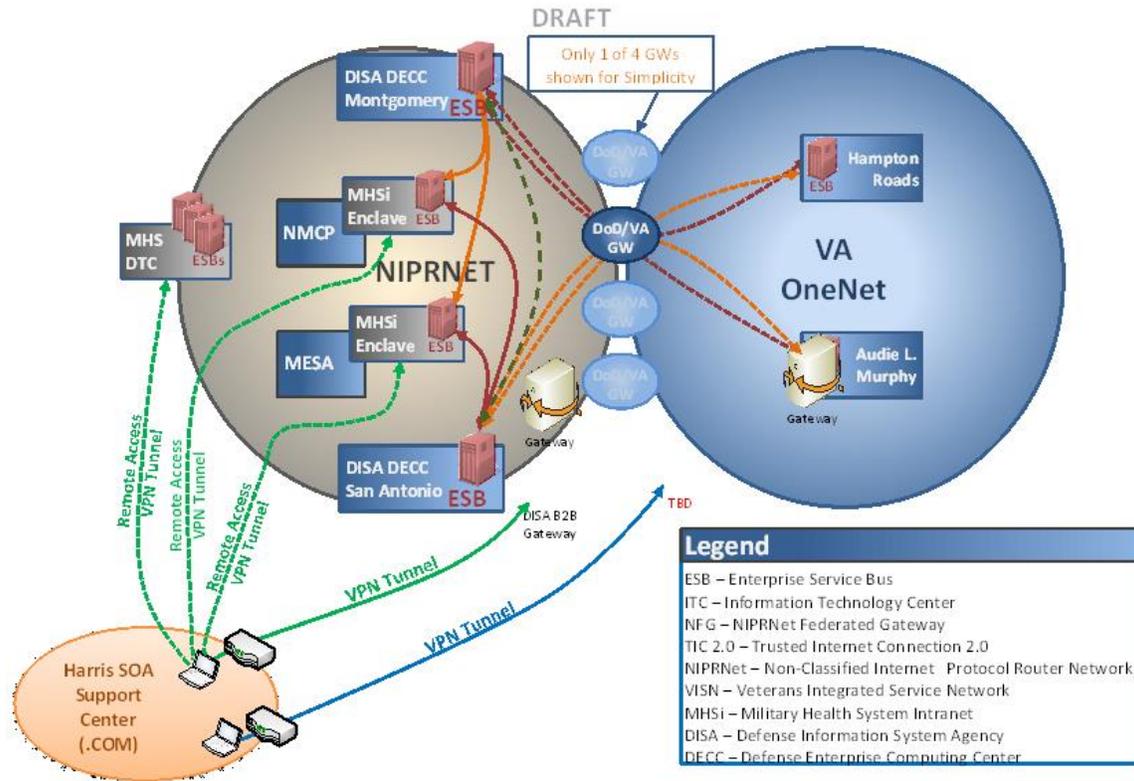


Figure 7 – Transition Network Connectivity

### 1-5.6.2 End State (Network Solution)

SOA/ESB infrastructure will be transitioned to Med-COI when it becomes available. Figure 8 shows the end state solution that will use the Med-COI network.

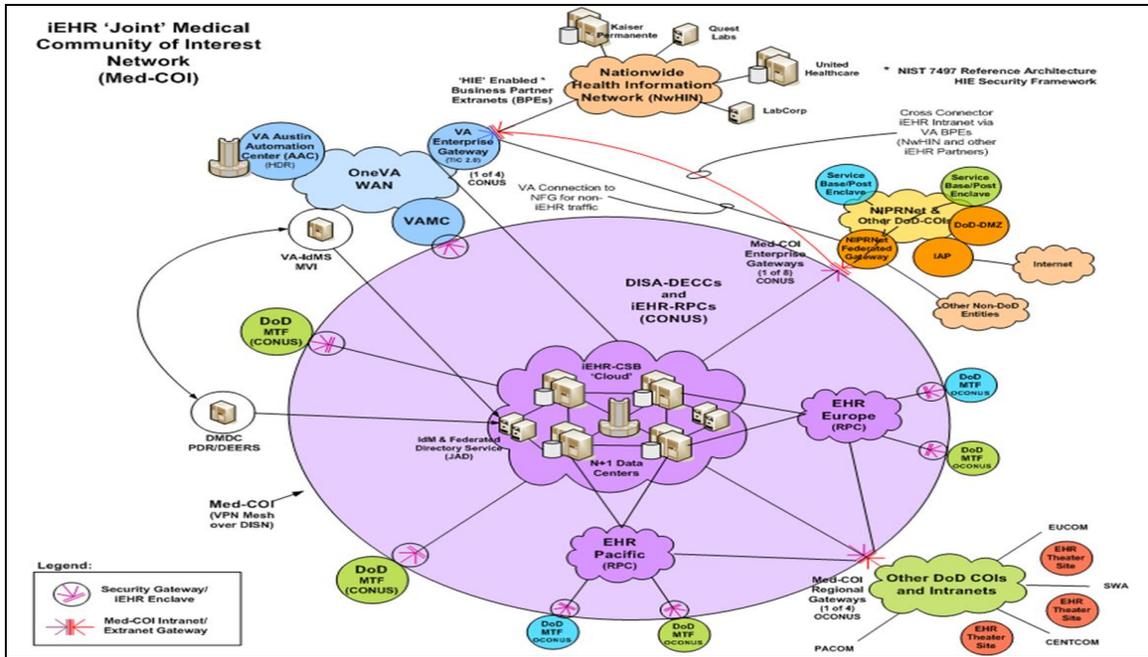


Figure 8 – End State Network Connectivity

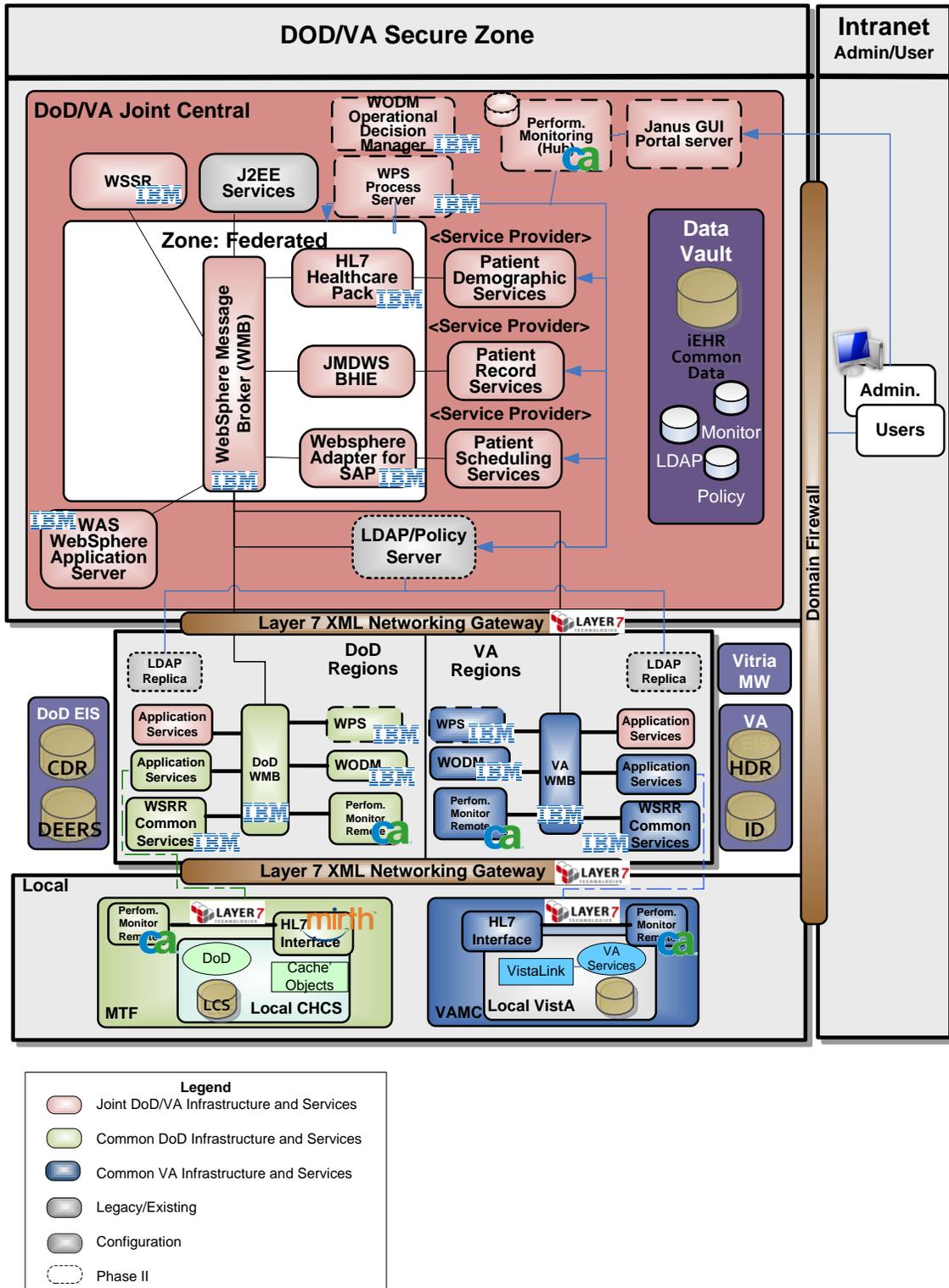


Figure 9 – DoD/VA Secure Zone

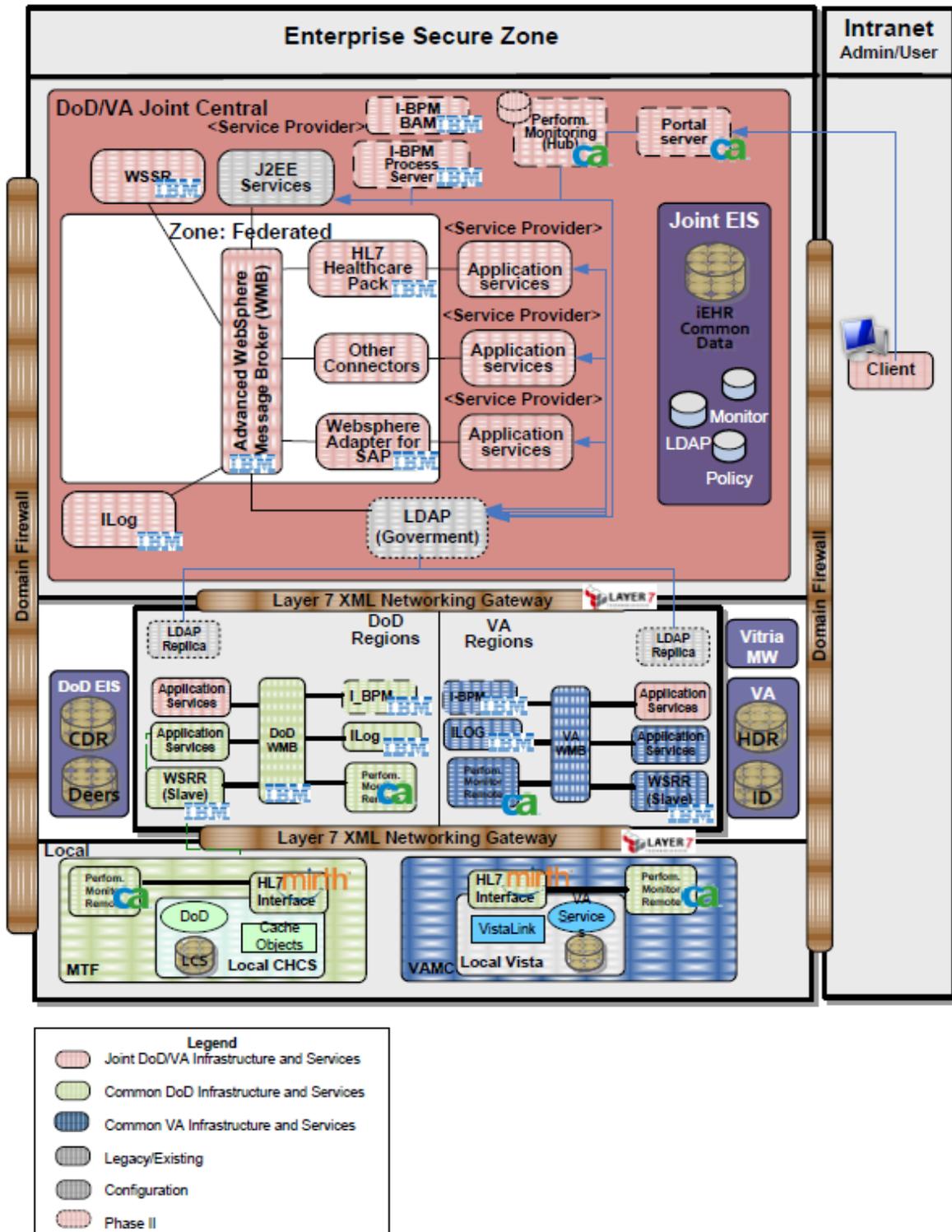


Figure 10 – Architecture Diagram Showing Software Components

## 1-5.7 Sandbox

The Harris SOA Suite solution is designed to provide comprehensive interface flexibility across the DoD/VA iEHR architecture. Two sandbox environments have been established for DoD/VA developers to develop trial integrations with the SOA Suite. These general and representative SOA Suite sandbox environments are available for third-party users and developers.

### 1-5.7.1 Contractor Sandbox Located at the Harris Melbourne Facility

The platform provided on this sandbox combines COTS ESB and COTS SOA ESB solutions at three levels of concern for the enterprise Military Health System (MHS) and VA software deployments. It is recommended for initial familiarity and training with SOA Suite products. It uses software components that will support monitoring, testing, and simulation configurations for the contractor-supported SOA sandbox environments providing access to DoD/VA product developers.

For guidance on how to gain access to this environment in order to develop, build, and maintain the work products associated with Development and Test Center (DTC) at MHS, please refer to SOA Suite Sandbox Appendix A - Contractor Sandbox. This document also provides the details about the physical and technical environment and a jumpstart kit with a reference implementation of a provider and consumer for the SOA Suite deployed.

Figure 11 shows the configuration of this sandbox.

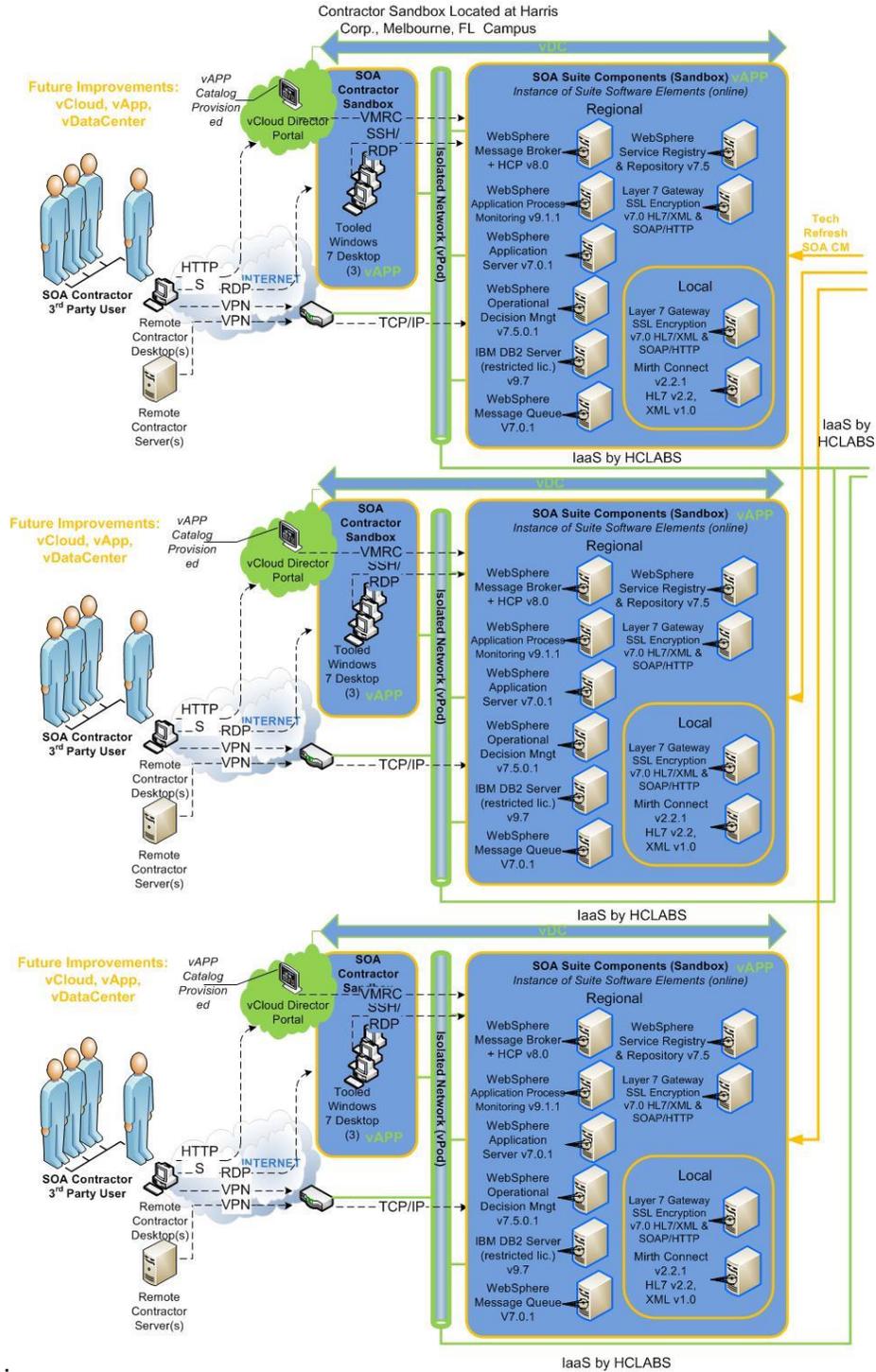


Figure 11 – Contractor Sandbox

## **1-5.7.2 Government Sandbox located at the JITC ITEC Maui, Hawaii Facility**

The Joint Interoperability Test Command (JITC) Integrated Test and Evaluation Center (ITEC) Maui, Hawaii Facility is a preferred developer's environment with other MHS-hosted enterprise applications. This sandbox will allow DoD/VA product developers to develop trial integrations with the SOA Suite. There will be two teams that support the SOA/ESB Suite engagement process on this sandbox. These teams will work in conjunction to provide a seamless test and development experience for third-party users. The two teams have separate, yet dependent roles in the support process. The teams will be referred to as the ITEC Support Team and the SOA/ESB Support Team. The SOA/ESB Support Team will work with the government to provide appropriate physical and remote access for government personnel, government furnished equipment (GFE) and government designated support contractors. The ITEC Team acts as approval authority for various activities among other responsibilities. For access and approval procedures, account setup and help desk information, please refer to SOA Suite Sandbox Appendix B – JITC ITEC Sandbox.

Figure 12 shows the configuration of the sandbox.

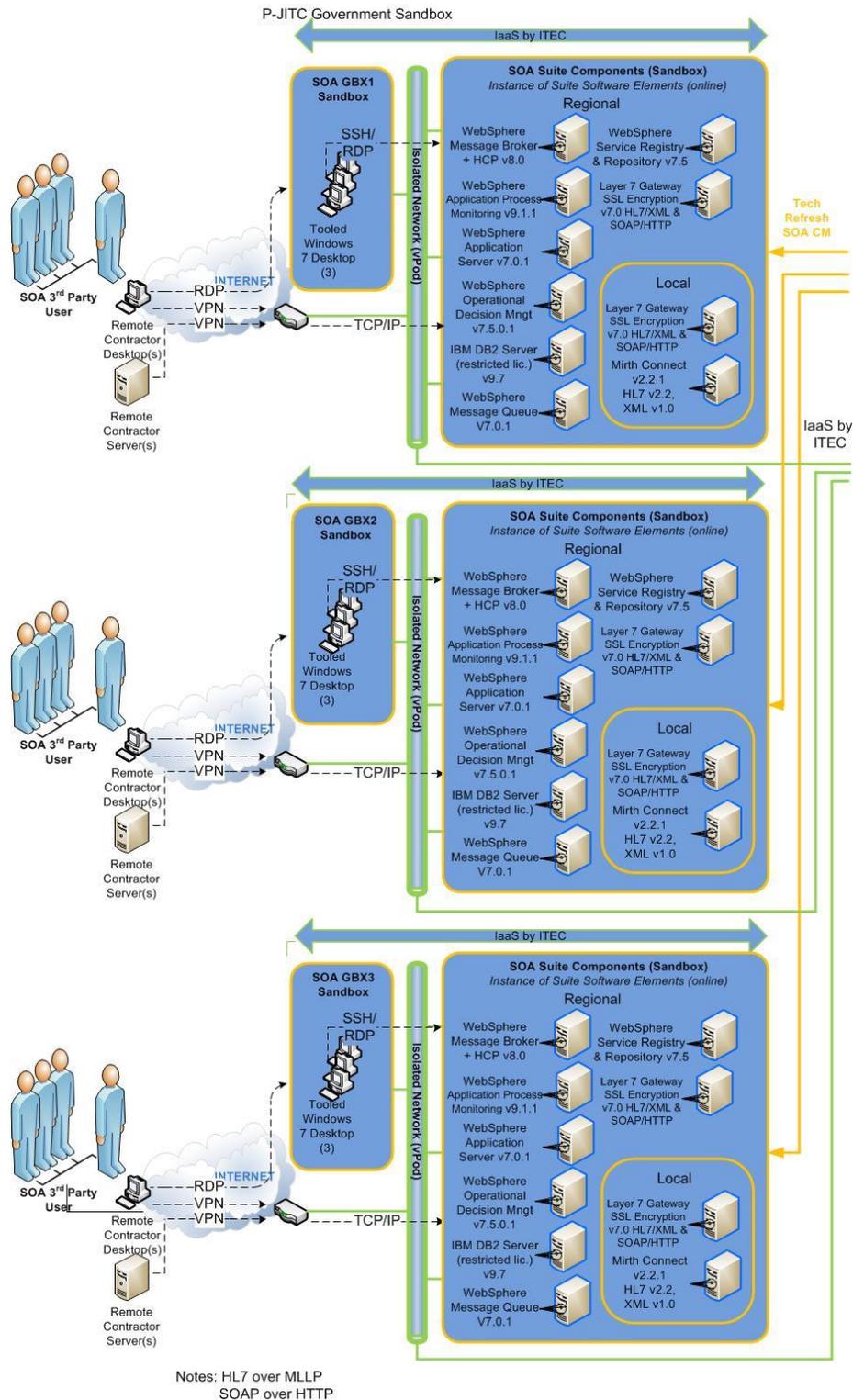


Figure 12 – Government Sandbox

All sandbox environments provide a basic SOA Suite with all the products to be used in the SOA Suite solution for the production environment (IBM WebSphere, Mirth, and Layer 7). Typically a SOA Suite environment will consist of the central/regional software stack and at least one local site.

### 1-5.7.3 Sandbox Access

The SOA Suite contractor team will coordinate and collaborate with the Government and third-party users to provide access to a representative set of SOA Suite products in the sandbox environments. The Government pre-approves all developers prior to beginning the SOA Suite sandbox on-boarding process. The contractor sandbox access is user-based and granted through a process of submitted authorization forms, approvals and access credentials passed to the requesting user. The current process is shown in Figure 13

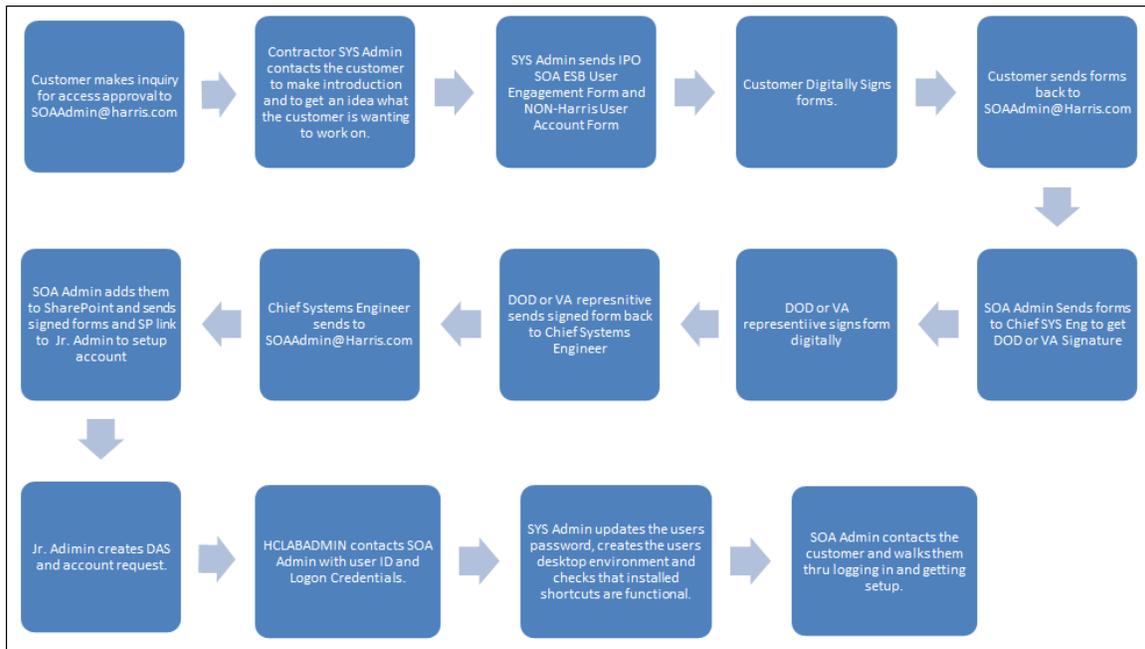
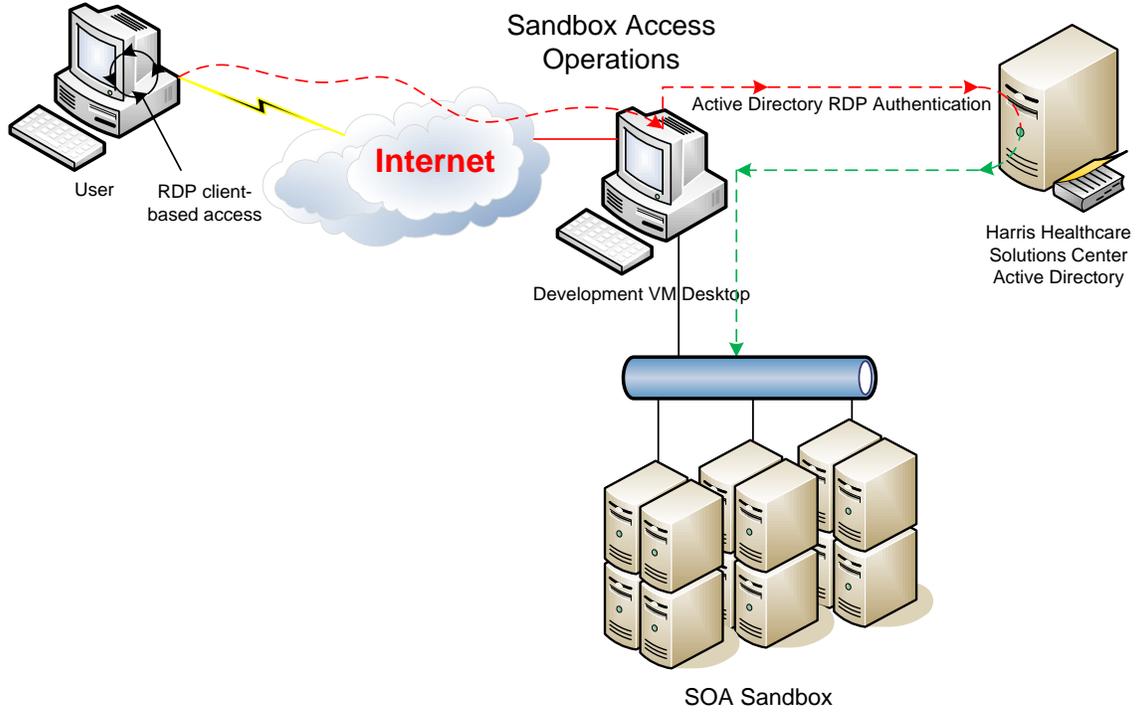


Figure 13 – Process Flow for Sandbox Access

#### 1-5.7.3.1 Access Methods

Access to the SOA Suite sandbox is available by two methods.

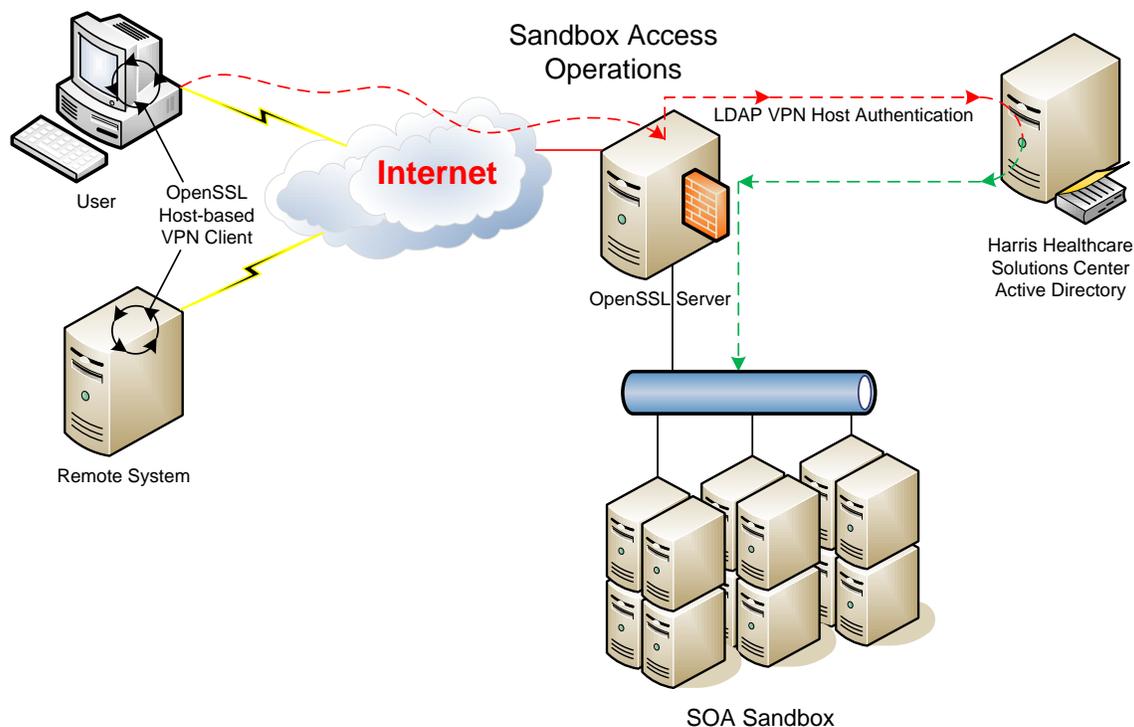
Method 1: Remote desktop protocol (RDP) to a development or test desktop that includes IBM WebSphere development tools or SOA test tools, as shown in Figure 14.



**Figure 14 – RDP Access**

Method 2: A host-based virtual private network (VPN) (secure socket layer (SSL) or Internet Protocol Security (IPSEC)) providing direct sandbox host(s) access via IP address, as shown in Figure 15.

The first of these methods assumes development or test to be contained within the sandbox, whereas the second assumes development or test and development/test tools reside on the host accessing over the VPN. Note that sandbox request gets a user into the sandbox space, though other credentialing may occur with the space at the system or services level.



**Figure 15 – VPN Access**

For further details on sandbox refer to SOA Suite Sandbox – SID 027.

## 1-5.8 Development and Test Environment (DTE)

The iEHR development and test environments will be designed to facilitate end-to-end system development and testing in an environment which closely reflects the field-level production system environments. The DTE will support the IPO product teams by providing environments and services that facilitate the development and testing of iEHR and Virtual Lifetime Electronic Record (VLER) capabilities and systems.

The environments are established to closely reflect field-level production system environments. The DTE will be a federated cloud-based environment that leverages a virtual collection of DoD/VA development and testing sites providing a unified set of capabilities and services for IPO customers. The MHS Development and Test Center (DTC), located in Richmond, Virginia, will serve as the “hub” of the DTE. This hub will serve as a gateway for new iEHR and VLER capabilities prior to their migration to a pre-production environment. An additional set of DoD/VA sites will provide a collection of capabilities, such as hosting of legacy applications to augment the capabilities of the DTC. The DTC will provide connectivity to these legacy applications. The DTC is not projected to house systems which contain “live” production patient data. The data sources available in a DTE are anticipated to contain “scrubbed” representative data suitable for use in a development environment.

Test Composite Health Care System (CHCS)/Armed Forces Health Longitudinal Technology Application (AHLTA) and Veterans Health Information Systems and Technology Architecture (VistA) systems with associated off-board servers supporting the interfaces, services and functional operation of the applications that will integrate with the SOA/ESB must be stood up and maintained by the respective contractor and vendors of these applications in order to perform system integration testing (SIT) and developmental test and evaluation (DT&E) testing events. For additional information about the plans for the DTE refer to Concept of Operations (CONOPS) Development and Test Environment (DTE) Version 1.0.

## 1-5.9 Quality Assurance Environment (Staging)

The quality assurance (QA) environment will be a scaled down mirror of production environment and will be hosted in the DTE. Services will be deployed on this environment after unit testing and this environment will be used for user acceptance testing (UAT), interoperability testing and regression testing.

At this time, there is no pre- production set up; therefore, the completed QA environment will be a replica of the sandbox environment.

## 1-5.10 Pre-production Environment

The pre-production environment will be an exact mirror of the production environment and will run the exact same code base as the production environment. After the service has been tested in the QA environment and certified as production deployable, the service will be deployed on the pre-production environment. In this environment, a performance baseline will be conducted to ensure that the newly deployed service will not impact performance. If any other certification is required for the service, it will be conducted in this environment prior to deployment in production.

## 1-5.11 Production

Production environment is elaborated in detail in section 1.1-5.3.

## 1-5.12 Failover and Load Balancing

Failover and load balancing are provided in two ways:

- Local and regional load balancers provided by existing GFE load balancing equipment. This is used for non-MQ traffic. Netscaler for Portsmouth & MESA.
- MQ provides failover and load balancing and will be used as the mechanism for MQ traffic.

GFE local load balancers must be configured to failover to backup regions in the event of lost communications.

- Regions are functionally the same – so one can failover to another.
- Each load balancer will have a “preferred” failover region to simplify configurations.
- In the event of total failure, inbound and outbound messages will be queued until communication is re-established.
- Queue size will be configured based on the traffic to store at least 48-hours of messages.

## 1-5.13 Disaster Recovery and Backup

System backups to tape are operationally not part of the SOA Suite system. However, SOA Suite system administrators will work with local DoD or VA system administrators to ensure all SOA Suite data is backed up. For further details on backups refer to SID\_045 Operations and Maintenance Plan - Section 4.9.1.

Most disaster recovery aspects are dependent upon network and hardware provider (e.g., backups, hardware redundancy, etc.). For further details refer to Contingency Operations Plan – SID 014.

## 1-6. SOI Role in the Service Life Cycle

The service life cycle processes are described in detail in Volume 2. SOA Suite infrastructure has a role in each of the life cycle phases. The life cycle phases are listed in **Error! Reference source not found..**

**Table 3 – SOI Role by Life Cycle**

Life Cycle Phase	SOI Role
Inception	Provide information about existing services and associated service level agreements. Provide information and guidance on infrastructure enhancements, if any.
Design	Provide information about existing infrastructure (Note: design standards are defined in SOA Volume 2)
Development	Provide access to sandbox and support if required
Testing	Perform service testing to ensure services comply with infrastructure standards and policies Produce test reports, certify the service is deployable
Deployment	Deploy services to production per instructions from development team Assist the development team to perform post deployment test, update registry and repository (WebSphere Service Registry and Repository (WSRR)).
Operations	Provide operations support and monitoring of infrastructure, Proactively trouble shoot any issues with network and infrastructure in regards to capacity, performance, security
Deprecation	Analyze impact on infrastructure
Retirement	Decommission the services and re-allocate infrastructure

## 1-7. Developer On-boarding Process (SOI Infrastructure)

A developer in this context refers to a programmer who is developing services related to iEHR that will be running on the SOA ESB and is assisting the deployment team in deploying these services on iEHR SOA sandbox/DTE or in production SOA environment.

A high-level process defining the steps from service request to implementation is provided in Volume 2: SOA Governance. This section illustrates the process after a service has been approved to be developed/integrated with the ESB.

This section illustrates steps to for on-boarding a new developer. A new developer would have to get the following to access to SOA suite. The assumption is that the developer would have a common access card (CAC) and GFE even though they are not required to develop the service. General requirements for a service developer to get access are listed below:

- **Access to sandbox** - Access to the sandbox is described in detail in section 1-5.7.3 of this document.
- **Access to DTE** - Access to DTE needs to be requested through a helpdesk ticket with appropriate approvals. Helpdesk process is described in detail in section 0 of this document.

The developers are expected to read through the three Governance documents, Volumes 1, 2 and 3, following understand and comply standards and processes in these documents.



Figure 17 shows the steps for on-ramping a service and the role played by various teams including the deployment team during this process. The process holds good for any services newly developed or any existing services undergoing enhancements.

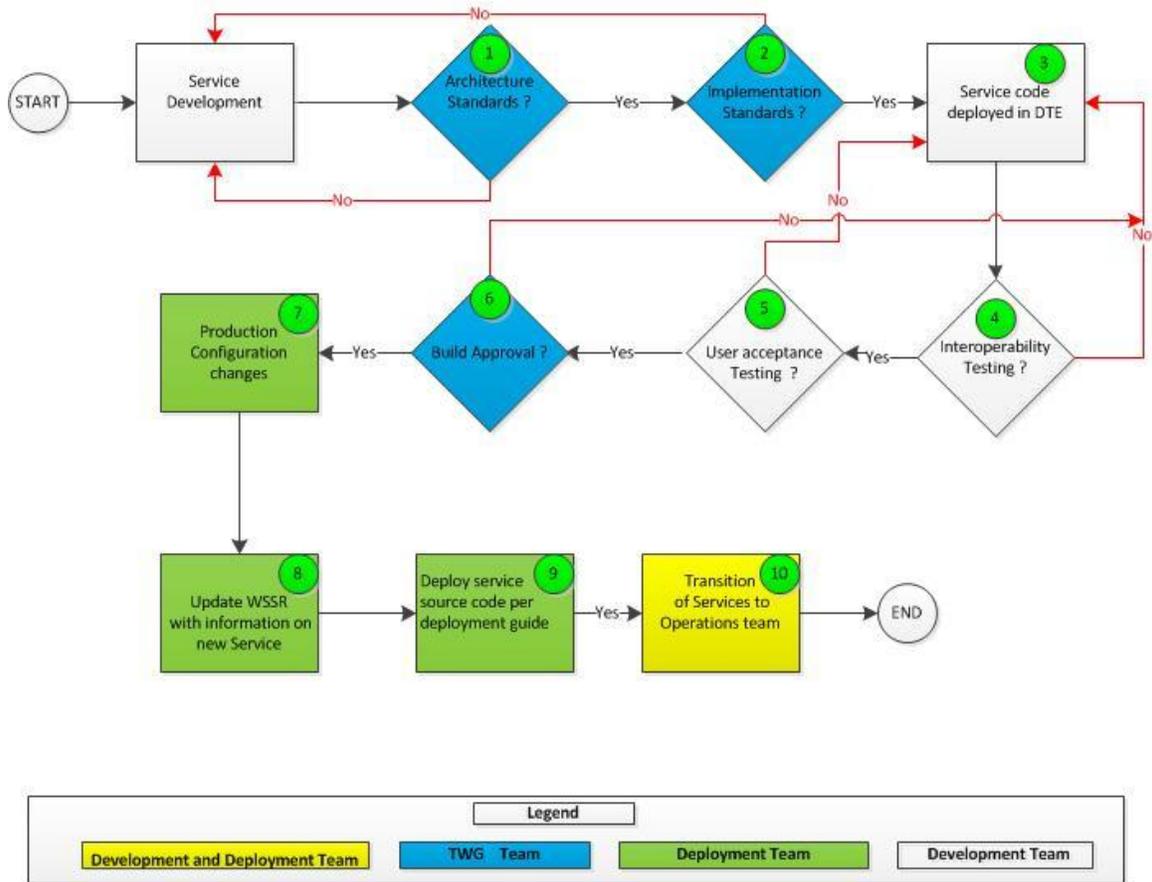


Figure 17 – SOI Role in Service On-Ramping

The workflow steps and actors involved in each step are explained in **Error! Reference source not found..** The applicable guidelines are contained in Volume 2 SOA Governance.

The table shows the workflow step corresponding to Figure 17, actors involved in that step of the workflow, description of the activities performed at that step and a list of applicable guidelines. The guidelines provide the entry and exit criteria and are defined in Volume 2 of SOA Governance document.

Table 4 – Service On-Ramping Process Workflow

Workflow Steps	Actor	Description	Applicable Guidelines
1	TWG Team	Confirm architecture standards are followed by the development team	SLM Design phase checklist
2	TWG Team	Confirm implementation standards (i.e. coding standards, naming convention etc.) are followed by the development team	SLM Construction phase checklist
3	Development Team	Migrate code from developer’s local environment to DTE.	NA
4	Development Team	Conduct Interoperability testing in DTE with assistance from deployment team	SLM Testing phase checklist
5	Testing Team and Development team	Conduct User Acceptance testing	SLM Testing phase checklist

Workflow Steps	Actor	Description	Applicable Guidelines
6	TWG Team and Operations Team	Conduct build and deployment review and approval	SLM Deployment phase checklist
7	Deployment Team	Perform Production configuration	SLM Deployment phase checklist
8	Deployment team	Promote WSSR changes from development instance to production WSSR	NA
9	Deployment team	Deploy the build into production environment	SLM Deployment phase checklist
10	Development team and Deployment team	Transition – Transition of service to operations team-	SLM Operational phase checklist

Any defects in a service under production will go through the normal incident management process described in the Operations and Maintenance Plan – SID 045. Any fixes to the services that does not result in a new version of the service will not be required go through the steps shown above. However, depending on the nature of the fix, a user acceptance test will be required before the service can be deployed in production.

### 1-8.2 Service Off-Ramping Process

Service off-ramping will be initiated by the service providers whenever they decide to retire the service or replace an existing service with a new service. This section assumes that the decision to deprecate and retire a process has been taken following the steps described in Section 2 under Service Lifecycle Management in Volume 2 SOA Governance.

The Figure 18 defines the workflow process of service off-ramping.

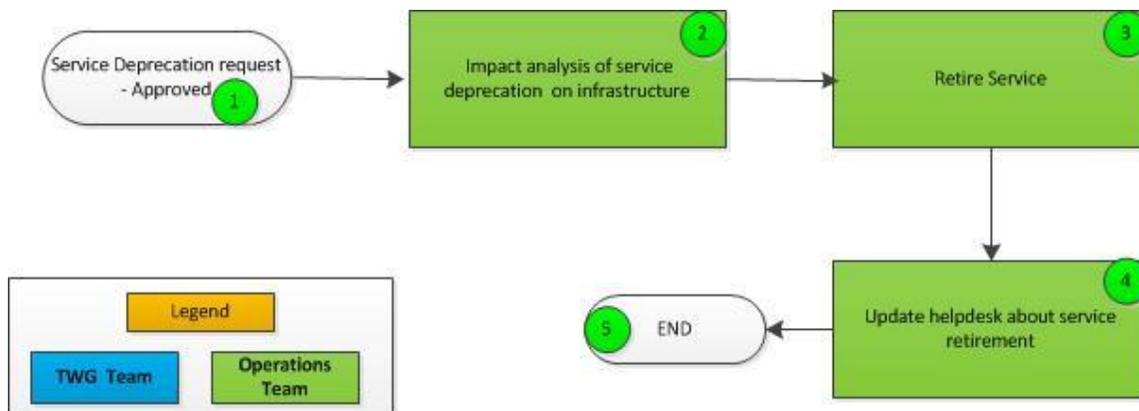


Figure 18 – Service Off-Ramping

The workflow steps and actors involved in every step are explained in **Error! Reference source not found.**

All the checklist guidelines are as per Volume 2 SOA Governance.

The table explains the workflow step corresponding to Figure 18, actors involved in that step of the work flow, description provides the activities performed at that step and checklist guidelines provide the entry and exit criteria defined in Volume 2 of SOA Governance document.

Table 5 – Service Off-Ramping Process Workflow

Workflow Steps	Actor	Description	Applicable Guidelines
----------------	-------	-------------	-----------------------

<b>Workflow Steps</b>	<b>Actor</b>	<b>Description</b>	<b>Applicable Guidelines</b>
1	TWG Team	Request for deprecation approval	SLM Deprecation phase checklist
2	Operations Team	Conduct impact analysis of service deprecation on infrastructure and deprecate the service	SLM Deprecation phase checklist
3	Operations Team	Retire the service	SLM Retired phase checklist
4	Operations Team	Confirm the Services are/is retired. Update WSSR and helpdesk.	SLM Retired phase checklist

## 1-9. Customer Support

CoE and SOA Suite will support the providers and consumers of the service using the iEHR SOA Suite. The level and type of support depends on the service life cycle phase. This section describes the SOA Suite support available for service providers and consumers.

### 1-9.1 Sandbox Support

SOA Suite team is responsible for all access, availability, and support of the two sandboxes. Service desk support will be available through a toll-free number. The service management process will be integrated with the DTE service desk processes. SOA Suite team will be responsible for issues related to SOA Suite COTS deployed in the six environments in the DTE.

### 1-9.2 General SOA Suite Support

SOA Suite support will provide Tier 3 support by integrating with the existing MHSSD and VA NSD customer facing Tier1 and Tier 2 support. A toll free number (888-906-2415) and email alias [SOASuite@harris.com](mailto:SOASuite@harris.com) has been established for this purpose. For further details on the support process refer to Operations and Maintenance Plan – SID 045.

### 1-9.3 Education and Training

SOA Suite team is developing curriculum and training development for the various components of the SOA Suite project. These are described in detail in the Training Program Plan – SID 043. Additionally, it provides more information about the training approach, type of training (e.g., instructor-led vs. electronic multi-media), roles and responsibilities, and the schedule.

For each SOA Suite capability, the SOA Suite support team will be developing and providing training materials, and services to include training on SOA management, integration and monitoring. Training will also include initial startup training at the sites where it is implemented and informal over-the-shoulder training on site after the installation.

Training for operations and maintenance (O&M) personnel shall be addressed during Operational Readiness Review and agreed upon by the Government. It is anticipated that new services will not require any training; however, major updates to the base operating system or SOA Suite components may require training.

For further details on the support process refer to Operations and Maintenance Plan – SID 045.

## 1-10. Configuration/Change Management

This section describes the configuration and change management process as it applies to SOA suite components and SOA suite infrastructure.

The change management related to services is described in Volume 2 SOA Governance.

To manage the identified software and non-software configuration items (CIs), the configuration management (CM) system is comprised of the following tool(s):

- Microsoft SharePoint
- Microsoft Team Foundation Server (TFS)

Together, the above tool(s) comprise the CM System and provide the following functionality:

- Provides access-controlled updates to CIs
- Store and retrieve all types of CIs, including software and non-software
- Store and retrieve CM records for CIs

The Configuration Management Compliance Plan – SID 011 describes in detail, configuration management plans and policies.

### 1-10.1 Change Requests

Changes to the SOA Suite, its operating environment and the supporting infrastructure will be managed by their respective configuration management tools and processes. The SOE CoE will primarily focus on governance of the iEHR SOA software services constituent to the Service Oriented Infrastructure (SOI). As iEHR SOA software services enter the operational phase they come under service configuration management, are recognized as part of the iEHR SOI and require formal change requests to be submitted to the SOE CoE for review and adjudication by the responsible iEHR organizational elements prior to operational release.

Any request for changes to hardware or software components (e.g., new services or change to existing services, new SOA suite component patches) will require approval from CoE. These request for changes after approval will provided to SOA Suite operations team to be executed.

## 1-11. Appendix A – Acronyms

Table 6 – Acronyms

Acronym/ Abbreviation	Description
CCB	Configuration Control Board
CM	Configuration Management
CMDB	Configuration Management Database
CoE	Center of Excellence
COTS	Commercial-Off-The-Shelf
CPU	Central Processing Unit
DECC	Defense Enterprise Computing Center
DIACAP	Defense Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoD SOEGC	DoD SOE Governance Council
DSL	Definitive Software Library
DTC	Development Test Center
DT&E	Development, Test, and Evaluation
EA	Enterprise Architecture
HER	Electronic Health Record
EHRWA	Electronic Health Record Way Ahead
ESB	Enterprise Service Bus
GB	Gigabyte
GFE	Government Furnished Equipment
HCP	Healthcare Connectivity Pack
HL7	Health Level 7
HW	Hardware
I-BPM	IBM Business Process Management System
IA	Information Assurance
iBRM	Integrated Business Reference Model
iEHR	Integrated Electronic Health Record
iLog	Business rule management and decision management system
IPO	Interagency Program Office
IS	Information Systems
IT	Information Technology
JGGB	Joint Government Governance Board
MESA	MHS Enclave, San Antonio, TX
MHS	Military Health System
MQ	Message Queue (IBM WebSphere Message Queue)
NAS	Network Attached Storage
NMCP	Naval Medical Center Portsmouth
O&M	Operations and Maintenance
ORR	Operational Readiness Review

Acronym/ Abbreviation	Description
OSI	Open System Interconnection
PMO	Program Management Office
RACI	Responsible, Accountable, Consulted, and Informed
RAID-5	Redundant Array of Independent Disks Level 5
RHEL	Red Hat Enterprise Linux
SAN	Storage Array Network
SD	Service Desk
SD&E	Service Design and Engineering
SID	Standard Item Deliverable
SLA	Service Level Agreement
SMEs	Subject Matter Experts
SOA	Service Oriented Architecture
SOE	Service Oriented Enterprise
SOI	Service Oriented Infrastructure
SSG	SecureSpan Gateway
SW	Software
TRR	Test Readiness Review
TWG	Technical Working Group
VA	Department of Veterans Affairs
VA ESS	VA Enterprise Shared Services
VAMC	Veterans Affairs Medical Center
VDP	vSphere Data Protection
VLER	Virtual Lifetime Electronic Record
VM	Virtual Machine
WAS	WebSphere Application Server
WMB	WebSphere Message Broker
WODM	WebSphere Operational Decision Management
WPS	WebSphere Process Server
WSRR	WebSphere Service Registry and Repository
XML	Extensible Markup Language

## 1-12. Appendix B – SOA Suite Component Descriptions

Detailed descriptions of SOA Suite software components are listed below.

- **WebSphere ESB** - The IBM WebSphere ESB stack supports the capabilities necessary to address the DoD and VA enterprise needs for deployment of a high-performance ESB into the central and regional systems. The core enterprise product at central and regional sites is the WebSphere Message Broker with the Healthcare Connectivity Pack. This ESB provides high-performance and high-function ESB services (Message Transformation and Routing) with healthcare extensions that include HL7 messaging, connectivity to most leading healthcare EHR systems, a standards-based canonical information model, etc. To provide open interfaces and extensibility, the local ESB solution is built on Mirth (messaging) and the Layer 7 networking gateway (security and lightweight ESB).
- **Mirth Connect** - Mirth Connect provides message-oriented and service-oriented integration for iEHR SOA Suite-ESB local sites. A standards-based healthcare integration engine facilitates the routing, filtering, and transformation of messages between health information systems over a variety of protocols.
- **Layer 7 SecureSpan Gateway** - The SOA Suite-ESB uses two interoperable components of the Layer 7 product suite that protects applications exposed as web services, connect applications across security and identity domains, and validate policy compliance across a transaction: SecureSpan Gateway (SSG) and the Layer 7 Policy Manager.

The SecureSpan Gateway is an XML firewall and service gateway designed to protect web services, accelerate XML operations, and mediate communications between SOA clients and services residing in different identity, security, or middleware domains.

Layer 7 Policy Manager is a GUI-based application that allows administrators to centrally define provision, verify, and audit fine-grained security and connectivity policies for cross-domain web services and XML integrations, on the Gateway.

- **WebSphere Message Broker (WMB) with Healthcare Connectivity Pack (HCP)** - WebSphere Message Broker is the core enterprise service bus for the DoD/VA Enterprise. The primary roles of WebSphere Message Broker within the SOA Suite-ESB are message routing, message transformation, message enrichment, and publish/subscribe.
- **WebSphere MQ (WMQ) (ECRC)** - WebSphere MQ provides message queuing infrastructure for the core SOA Suite-ESB. MQ Server provides the basic message queuing infrastructure for the core SOA Suite-ESB at the regional and central sites. MQ can provide encrypted channels, but we will be relying on Layer 7 appliances/virtual appliances to perform this function in the SOA Suite-ESB architecture.
- **WebSphere Registry and Repository (WSRR)** - WebSphere Service Registry and Repository (WSRR) is the master metadata repository for service descriptions.
- **WebSphere Business Monitor (WBM)** - WebSphere Business Monitor provides an up to date view of business performance. It provides predictions so that you can take action before process problems occur. Personalized business dashboards process business events and data, and calculate key performance indicators (KPIs) and metrics.
- **WebSphere Operational Decision Management (WODM) formerly known ILOG** - WebSphere Operational Decision Management (WODM) application server provides the automation and governance of frequently occurring repeatable decisions that control the actions critical business systems. Improves the quality of each customer, partner, or internal interactions and drive more actions that are responsive to business opportunities or risk conditions.
- **WebSphere Transformation Extender (WTX) with Healthcare Pack** - WebSphere Transformation Extender (WTX) (for Integration Servers), the associated WTX HealthCare Packs, and the WTX Design Studio provide support for the HIPAA EDI formats and the NCPDP formats,

and the tooling to support mapping from those formats to other data formats. For the purposes of the SOA Suite, WTX is included as a node for use with WebSphere Message Broker. This enables Message Broker to work with the formats referenced above.

- **WebSphere Process Server (WPS) IBM** - IBM Business Process Manager Advanced offers the complete set of advanced BPM capabilities. It extends the support for high-volume process automation, with high quality-of-service.
- **WebSphere Application Server Network Deployment (WAS ND)** - IBM WebSphere Application Server is the leading software foundation for service-oriented architecture (SOA) applications and services for the enterprise.
- **DB2 Database Management System** - DB2 provides database support central to the SOA Suite-ESB of applications for the Regional implementations of the SOA Suite-ESB.

For further details on software components, configuration, security policies related to software refer to Security Management Plan – SID 046.

## 1-13. Appendix C – Error Message References

This appendix provides documentation for error message facilities for all SOA Suite COTS products.

It includes reference information for error messages generated by a number of the COTS products used in the iEHR SOA Suite. This document focuses on the CA Application Performance Management (APM) toolset, which is used to monitor the health and performance of the SOA Suite, and the products that comprise the Enterprise Service Bus (ESB), including:

- Mirth Connect
- Layer 7 Secure Span Gateway
- IBM WebSphere Message Broker
- CA APM

The references in this appendix are intended to assist:

1. A developer or integrator of iEHR services, who will be “connecting to the bus” by interfacing a service directly with one of the three products that comprise the ESB (Mirth, Layer 7, and Message Broker). References contained in this document include information regarding:
  - Error messages or exceptions that may be sent from the ESB to a connected service
  - Error messages that a user of integration toolsets provided by the products may encounter.
2. A Helpdesk support technician, who is responsible for troubleshooting error messages or alerts from APM.

### 1-13.1 Background

Many of the SOA suite errors will not reach the end users of the application users. The end users will only see the results of the initial error. For example, if a message is not received at a destination, the developer will see that an HL7 message did not reach its intended destination. Then the help desk will need to know how to first find the reference to this error in the COTS documentation, then troubleshoot this error message. This also involves some ack/nack messages that come right off the ESB from message generators, that a message either was not sent or not received.

### 1-13.2 Custom Error Messages

Ultimately, the iEHR SOA Suite project team can define and control error messages that are returned from the ESB to a connected service or a connected consumer. While the ESB can respond with “out of the box” error messages, each component of the ESB allows for the customization of these error messages. This means the iEHR SOA Suite project team could define what error messages were returned to services for specific situations. Additionally, error handling flows allow integrators to define how error messages are handled and routed by the ESB.

Similarly, the CA APM toolset allows administrators to define application and situation specific error messages, and determine when they are thrown by agents installed on SOA Suite components.

The following assumptions apply to this appendix

The assumptions, this document is based on, are:

- This is for all potential error messages, for all COTS tools.
- This reference is for the Tier 1 government staffed help desk.
- These are errors only the developers and integrators will see (not the application users).

- Some users may see an alert, because of a performance impact, but not be an actual error message.

### 1-13.3 COTS Error Message – References

Below is a listing of web site links, where available, to vendor web sites for their COTS error messages documentation.

WebSphere Message Broker (WMB) errors refer to the following URLs for reference information regarding IBM WebSphere Message Broker error messages:

- [Handling Timeout Notification errors](#)
- [Handling exceptions in aggregation flows](#)
- [Reason Codes](#)
- [Resolving problems that occur during deployment of message flows](#)
- [Diagnostic Messages](#)
- [Error messages for troubleshooting](#)

WebSphere MQ (WMQ) Errors:

- [Handling MQ Input Errors](#)
- [http://publib.boulder.ibm.com/infocenter/wmqv7/v7r0/index.jsp?topic=%2Fcom.ibm.mq.csqsao.doc%2Ffm12030\\_1.htm](http://publib.boulder.ibm.com/infocenter/wmqv7/v7r0/index.jsp?topic=%2Fcom.ibm.mq.csqsao.doc%2Ffm12030_1.htm)

WebSphere Process Manager (WPM) Errors:

- <http://www-01.ibm.com/support/docview.wss?uid=swg27037045>

WebSphere Process Server (WPS) Errors:

- [http://www-947.ibm.com/support/entry/portal/problem\\_resolution/software/websphere/websphere\\_process\\_server](http://www-947.ibm.com/support/entry/portal/problem_resolution/software/websphere/websphere_process_server)

WebSphere Service Registry and Repository (WSRR) Errors:

- [http://publib.boulder.ibm.com/infocenter/sr/v7r0/index.jsp?topic=%2Fcom.ibm.sr.doc%2Fcwsr\\_troubleshootingandsupport.html](http://publib.boulder.ibm.com/infocenter/sr/v7r0/index.jsp?topic=%2Fcom.ibm.sr.doc%2Fcwsr_troubleshootingandsupport.html)

WebSphere Operational Decision Management (WODM) Errors:

- [http://pic.dhe.ibm.com/infocenter/dmndhelp/v7r5mx/index.jsp?topic=%2Fcom.ibm.ws.icp.hccpay.doc%2Fhc%2Fpayor%2Fpayordev%2Freference%2Ftr\\_trblsht.html](http://pic.dhe.ibm.com/infocenter/dmndhelp/v7r5mx/index.jsp?topic=%2Fcom.ibm.ws.icp.hccpay.doc%2Fhc%2Fpayor%2Fpayordev%2Freference%2Ftr_trblsht.html)
- [http://pic.dhe.ibm.com/infocenter/dmanager/v8r0m1/index.jsp?topic=%2Fcom.ibm.wodm.dserver.events.dev%2Ftopics%2Ftsk\\_dse\\_busruleconnect\\_troubleshoot.html](http://pic.dhe.ibm.com/infocenter/dmanager/v8r0m1/index.jsp?topic=%2Fcom.ibm.wodm.dserver.events.dev%2Ftopics%2Ftsk_dse_busruleconnect_troubleshoot.html)
- [http://pic.dhe.ibm.com/infocenter/dmanager/v8r0m1/index.jsp?topic=%2Fcom.ibm.wodm.family.troubleshooting%2Ftopics%2Fcon\\_support\\_troubleshoot.html&resultof%3D%2522%2574%2572%](http://pic.dhe.ibm.com/infocenter/dmanager/v8r0m1/index.jsp?topic=%2Fcom.ibm.wodm.family.troubleshooting%2Ftopics%2Fcon_support_troubleshoot.html&resultof%3D%2522%2574%2572%)

[http://pic.dhe.ibm.com/infocenter/dmanager/v8r0m1/index.jsp?topic=%2Fcom.ibm.wodm.family.troubleshooting%2Ftopics%2Fcon\\_support\\_resources.html&resultof%3D%2522%2574%2572%256f%2575%2562%256c%2565%2573%2568%256f%256f%2574%2569%256e%2567%2522%2520%2522%2574%2572%256f%2575%2562%256c%2565%2573%2568%256f%256f%2574%2522%2520](http://pic.dhe.ibm.com/infocenter/dmanager/v8r0m1/index.jsp?topic=%2Fcom.ibm.wodm.family.troubleshooting%2Ftopics%2Fcon_support_resources.html&resultof%3D%2522%2574%2572%256f%2575%2562%256c%2565%2573%2568%256f%256f%2574%2569%256e%2567%2522%2520%2522%2574%2572%256f%2575%2562%256c%2565%2573%2568%256f%256f%2574%2522%2520)

- [http://pic.dhe.ibm.com/infocenter/dmanager/v8r0m1/index.jsp?topic=%2Fcom.ibm.wodm.family.config.was%2Fshared\\_config\\_websphere\\_topics%2Ftpc\\_ws\\_res\\_troubleshooting.html&resultof%3D%2522%2574%2572%256f%2575%2562%256c%2565%2573%2568%256f%256f%2574%2569%256e%2567%2522%2520%2522%2574%2572%256f%2575%2562%256c%2565%2573%2568%256f%256f%2574%2522%2520](http://pic.dhe.ibm.com/infocenter/dmanager/v8r0m1/index.jsp?topic=%2Fcom.ibm.wodm.family.config.was%2Fshared_config_websphere_topics%2Ftpc_ws_res_troubleshooting.html&resultof%3D%2522%2574%2572%256f%2575%2562%256c%2565%2573%2568%256f%256f%2574%2569%256e%2567%2522%2520%2522%2574%2572%256f%2575%2562%256c%2565%2573%2568%256f%256f%2574%2522%2520)
- [http://pic.dhe.ibm.com/infocenter/dmanager/v8r0m1/index.jsp?topic=%2Fcom.ibm.wodm.family.config.was%2Fshared\\_config\\_websphere\\_topics%2Ftpc\\_ws\\_res\\_troubleshooting.html&resultof%3D%2522%2574%2572%256f%2575%2562%256c%2565%2573%2568%256f%256f%2574%2569%256e%2567%2522%2520%2522%2574%2572%256f%2575%2562%256c%2565%2573%2568%256f%256f%2574%2522%2520](http://pic.dhe.ibm.com/infocenter/dmanager/v8r0m1/index.jsp?topic=%2Fcom.ibm.wodm.family.config.was%2Fshared_config_websphere_topics%2Ftpc_ws_res_troubleshooting.html&resultof%3D%2522%2574%2572%256f%2575%2562%256c%2565%2573%2568%256f%256f%2574%2569%256e%2567%2522%2520%2522%2574%2572%256f%2575%2562%256c%2565%2573%2568%256f%256f%2574%2522%2520)

#### WebSphere Application Server (WAS) Errors:

- [http://www-947.ibm.com/support/entry/portal/problem\\_resolution/software/websphere/websphere\\_application\\_server](http://www-947.ibm.com/support/entry/portal/problem_resolution/software/websphere/websphere_application_server)

#### DataBase 2 (DB2):

- <http://www-01.ibm.com/support/docview.wss?uid=swg27010211>
- [http://www-947.ibm.com/support/entry/portal/problem\\_resolution/software/information\\_management/db2\\_query\\_management\\_facility](http://www-947.ibm.com/support/entry/portal/problem_resolution/software/information_management/db2_query_management_facility)

## 1-14. References

1. SOA Services Governance Volume 2
2. The Open Group Service Integration Maturity Model, Open Group 2009.
3. Service Oriented Architecture Suite Performance Work Statement, August 2011
4. iEHR CDR SOA Suite 2013
5. Configuration Management Compliance Plan – SID 011
6. Operations and Maintenance Plan – SID 045
7. Security Management Plan – SID 046
8. SOA Suite Sandbox Appendix A – Contractor Sandbox – SID 027
9. SOA Suite Sandbox Appendix B – JITC ITEC – SID 027
10. Concept of Operations (CONOPS) Development and Test Environment (DTE), November 2012