

U.S. DEPARTMENT OF VETERANS AFFAIRS

Office of Information and Technology



Enterprise Technology Strategic Plan, Fiscal Year 2017-2021

March 8, 2016

THIS PAGE INTENTIONALLY LEFT BLANK FOR PRINTING PURPOSES

APPROVAL COORDINATION



Digitally signed by Rodney J. Emery 106229
DN: dc=gov, dc=va, o=internal, ou=people,
0.9.2342.19200300.100.1.1=rodney.emery@va.gov, cn=Rodney J.
Emery 106229
Reason: I have reviewed this document.
Date: 2016.03.24 19:43:53 -0400

Rodney Emery
Director, Technology Strategies and GEAC, ASD
ASD Technology Strategies

PAUL A. TIBBITS
116858

Digitally signed by PAUL A. TIBBITS 116858
DN: dc=gov, dc=va, o=internal, ou=people,
0.9.2342.19200300.100.1.1=paul.tibbits@va.gov, cn=PAUL A. TIBBITS
116858
Reason: I am approving this document.
Date: 2016.03.31 16:13:48 -0400

Paul A. Tibbits, M.D.
DCIO Architecture, Strategy, and Design

TABLE OF CONTENTS

EXECUTIVE SUMMARY	6
1 INTRODUCTION	7
1.1 Business Drivers Influencing IT Planning	7
1.2 Current Environment.....	14
1.3 IT Services and Capabilities	15
2 ANALYSIS OF CURRENT ENVIRONMENT	16
3 TRANSITION ACTIVITIES TO ADDRESS INFRASTRUCTURE GAPS.....	17
3.1 Infrastructure Gaps.....	17
4 FUTURE ENVIRONMENT	20
4.1 VA IT Vision.....	20
4.2 Transition Activities for Cloud Computing & Infrastructure Gaps.....	25
4.3 Transition Activities to Address Security Gap.....	29
4.4 Transition Activities to Address Information Management Gap.....	35
4.5 Transition Activities to Address Interoperability Gap	37
4.6 Transition Activities to Address Mobile Gaps.....	41
4.7 Transition Activities to Address Application Modernization Gap	43
4.8 Transition Activities to Address Collaboration Gap.....	45
4.9 IT Consolidation Efforts	47
5 VA PROCESSES SUPPORTING TRANSITION	49
5.1 Enterprise Technical Architecture Compliance Criteria	50
5.2 Technical Reference Model	50
5.3 Enterprise Design Patterns	51
5.4 Enterprise Management Framework	52
5.5 IT Governance.....	53
6 IMPACTS ON IT TRANSITION EFFORTS.....	53
6.1 Technology Trends	54
6.2 Legal Factors	60
7 CONCLUSION.....	60
APPENDIX A: INTERIM IT VISION (3-YEAR).....	62
1. USERS/DEVICES:	63
2. APPLICATIONS:.....	64
3. SERVICES:	66
4. INFRASTRUCTURE:.....	70
APPENDIX B: STATUTORY, REGULATORY AND GUIDANCE FACTORS	74
APPENDIX C: BIBLIOGRAPHY.....	79
APPENDIX D: ACRONYMS	82

TABLES:

Table 1: MyVA Workstreams and VA Strategic Plan Alignment 10

Table 2: Additional Business Drivers of VA Infrastructure 12

Table 3: OI&T Services and Capabilities 16

Table 4: Infrastructure Gaps and Future State for each Capability 18

Table 5: Transition Activities and Enterprise Design Patterns Alignment 19

Table 6: Attributes of Future Environment 25

Table 7: Enterprise Design Pattern 52

FIGURES:

Figure 1: MyVA Task Force Workstream Transition 9

Figure 2: OI&T's Strategic Framework 13

Figure 3: Current VA IT Environment 15

Figure 4: VA IT Vision Diagram 21

Figure 5: VA Enterprise Technical Architecture (ETA) Compliance 50

Figure 6 – Interim IT Vision (3-Year) 62

EXECUTIVE SUMMARY

The Enterprise Technology Strategic Plan (ETSP) charts the strategy to achieve the Information Technology (IT) vision for the Department of Veterans Affairs (VA). The IT vision is to lead VA as *a world-class organization that provides a seamless, unified Veteran experience through the delivery of state-of-the-art technology*. The ETSP aligns with the VA mission, the VA core values, and the MyVA continuous improvement initiative. The plan sets priorities, focuses energy and resources, strengthens VA IT operations, and ensures that VA stakeholders are working toward common goals and intended outcomes that best serve our Nation’s Veterans.

The purpose of the ETSP is to guide enterprise-wide IT planning and decision-making. The ETSP directs leaders of the Architecture, Strategy, and Design (ASD) pillar of the VA Office of Information and Technology (OI&T) to act as stewards of VA IT resources to identify and articulate the requirements, standards, and opportunities for transformative technology improvements. As required by the White House Office of Management and Budget (OMB), ETSP also serves as a source for the IT infrastructure Service Delivery section of the Enterprise Roadmap to document VA’s transformation activities.

The ETSP describes the current “As Is” state of the VA IT infrastructure by evaluating current business drivers that influence IT planning. The ETSP also defines the future “To Be” state of the IT infrastructure, with plans to provide internal users and mission partners with a robust, agile, secure, and interoperable framework. This enterprise architecture will enable connectivity, computing capabilities, and appropriate methodologies for the delivery of integrated services to Veterans. And while OI&T currently responds to the VA mission by providing adequate services and capabilities to its customers, the ETSP notes the existence of significant opportunities for improvement in the infrastructure. The ETSP demonstrates support for the ASD commitment to transparency and the elimination of material weaknesses.

The ETSP assesses the impact of specific innovations and projects to transform future VA operations. These include current and planned migration activities, such as the transition from the use of the Project Management Accountability System (PMAS) to the more agile and flexible project management process, the Veteran-focused Integration Process (VIP). The VIP deployment is scheduled to begin on April 1, 2016, with implementation for existing projects to begin in Fiscal Year (FY) 2017. Thus, some details of the activities presented in the ETSP are in a state of transition; transformations which may ensue will be reflected in the next iteration of the ETSP in FY17, and annually, thereafter.

The ETSP recommends and describes the implementation of technological advancements that provide significant solutions to the challenges facing the VA IT infrastructure, in order to ensure VA mission success.

1 INTRODUCTION

VA OI&T provides strategic, technical, and customer-service direction, guidance, and policy to ensure VA mission outcomes in the delivery of integrated IT services to VA stakeholders. OI&T seeks to build a VA IT infrastructure that is robust, adaptive, agile, secure, interoperable, and cost-effective.

To support the MyVA continuous service culture, OI&T and its pillars have employed transformative actions that provide a more people-centric, results-oriented, and progressive IT infrastructure. To achieve its mission, OI&T has undertaken multiple enterprise level initiatives, such as Enterprise Shared Services (ESS), upgraded information assurance and security, enhanced support for mobile users, and cloud services. These developments comprise the critical foundation that enable Veteran-facing initiatives.

The ASD pillar of VA OI&T is responsible for managing and creating standards for implementing IT solutions that serve Veterans. Within the ASD pillar, the Office of Technology Strategies (TS) partners with OI&T customer pillars and advocates to develop the ETSP to achieve the enterprise technology vision for VA. The plan includes enterprise-wide IT strategies, models, and standards that comprise the technology layer of the One VA Enterprise Architecture (EA).

TS also partners with industry and other government agencies to leverage existing enterprise technologies and best practices to demonstrate strategic IT value. As a result, TS provides stakeholders with comprehensive information about OI&T strategies, such as the use of technologies, tools, and Enterprise Design Patterns, to meet OI&T and VA goals and objectives.

1.1 Business Drivers Influencing IT Planning

The purpose of integrating IT in business solutions is to enable VA to optimize its performance in meeting its mission. Many VA programs rely heavily on IT to deliver comprehensive health and benefit services to our Nation's Veterans, and to ensure that information is shared seamlessly with the Department of Defense (DoD) and other partners. Therefore, as VA identifies key drivers behind agency-wide strategic planning efforts, OI&T must ensure that strategic planning, budgeting, and investment guidance will align with VA's Strategic Plan.

1.1.1 MyVA Task Force

As an organization, VA currently functions within a transitional period of complex business conversions as it refocuses its mission. Beginning in September 2014, the Secretary of VA established a MyVA Task Force to plan a Veteran-centric operational transformation. The Task Force established a national network of Community Veteran Advisory Councils to coordinate service delivery with local, state, and community partners. The Task Force examined the best methods to realign internal business processes, using a shared services model that enables VA

organizations to leverage support services to improve efficiency, reduce costs, and increase productivity.

A significant MyVA effort promotes a unified Veteran experience by streamlining digital assets. VA is transitioning existing websites and web services to a single website that runs on desktops, tablets, kiosks, and mobile devices. The website will be operated by the Veterans Experience Office and the web address will be determined by feedback from Veterans.¹ Three main MyVA drivers include:

- **Single Face to the Customer:** VA websites that provide services to Veterans will be designed and engineered to provide a single interface to Veterans. Veterans will be able to navigate through the full range of available VA services from this single website. This capability will be supported by a Single Sign-on (SSO) capability, so that Veterans will not be required to remember multiple usernames and passwords.
- **Common Customer Data:** Core data elements, such as identity, military service record, and contact information, will be normalized across the enterprise, since they are necessary for interaction with Veterans. Authoritative sources for Common Customer Data (CCD) will be identified, and services that provide access and update capabilities for CCD will be developed. The sources and services will be made available to VA application software for implementation.
- **Optimized IT Service Delivery:** The delivery of IT services will be enhanced to ensure that VA employees are appropriately empowered to accomplish the VA mission objectives. Employee decision-making authorization will be realigned to support the recent regional realignment for the delivery of services to Veterans. This action optimizes where, and by whom, the decisions are made within VA.

In 2016, new Agency Priority Goals will be established that reflect MyVA priorities. In the meantime, VA organizations will continue to document their outcomes, programs, budgets, and plans to achieve the MyVA vision. This includes the ETSP and other plans, such as the VA Strategic Plan, Information Resource Management Strategic Plan, and the Enterprise Roadmap.

When the long-term requirements and interdependencies are fully understood and defined, Task Force resources and responsibilities will be realigned and transitioned to permanent entities within VA, in order to implement and institutionalize the MyVA concepts. Figure 1 provides a notional view of how Task Force responsibilities might be transitioned to existing organizations within VA.

¹ Memorandum: VA Regional Alignment. Department of Veterans Affairs Chief of Staff. January 26, 2015. <http://afgenvac.org/wp-content/uploads/2015/01/VA-Regional-Alignment-Memo-Single-VA-Website-Memo.pdf>

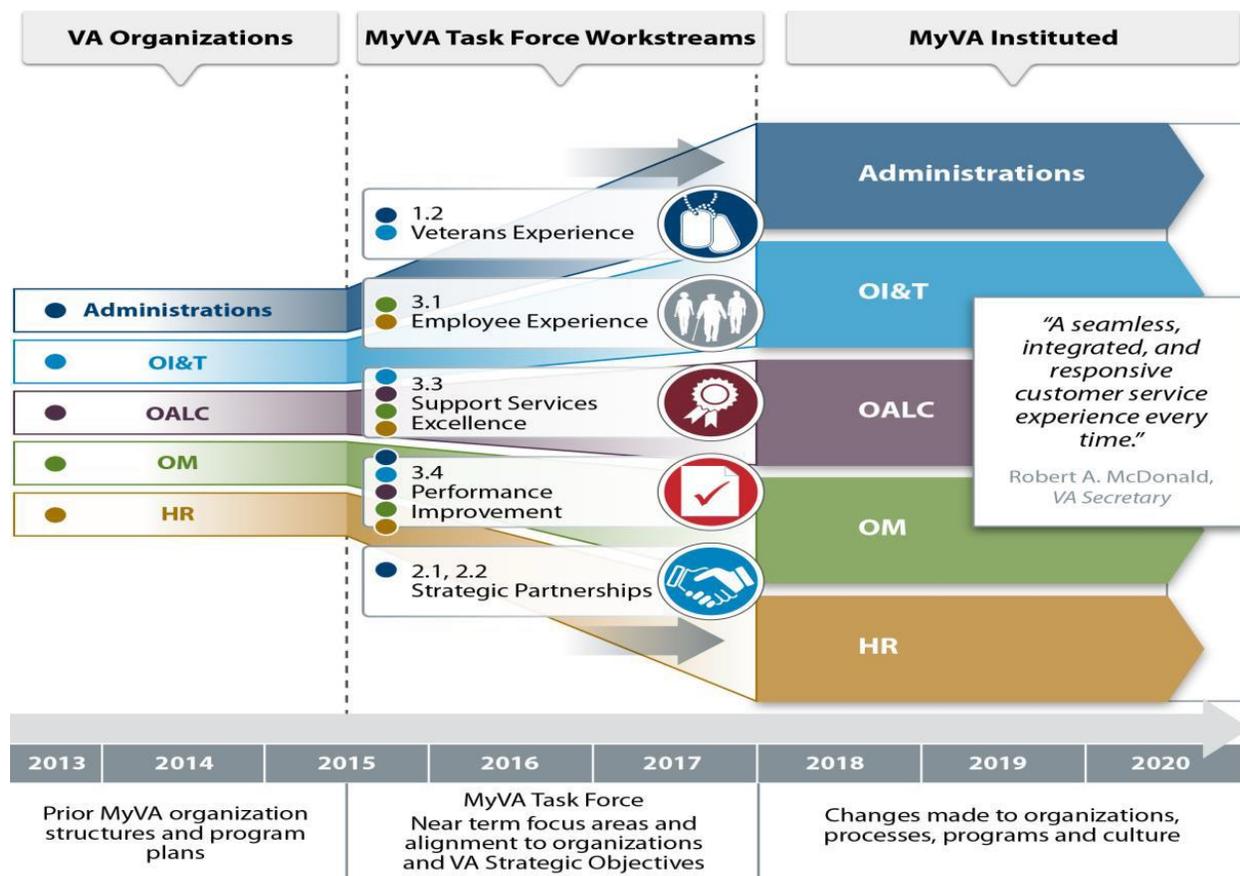


Figure 1: MyVA Task Force Workstream Transition²

Current MyVA Task Force workstreams, their missions, the FY2015 – 2016 goals, and alignment to the FY2014 – 2020 VA Strategic Plan are summarized in Table 1.

² FY 2013-2015 Enterprise Roadmap Addendum. Department of Veterans Affairs. May 29, 2015. http://www.ea.oit.va.gov/EAOIT/docs/May_2015-Release_Documents/VAFY13-15EnterpriseRoadmapAddendum.pdf

Table 1: MyVA Workstreams and VA Strategic Plan Alignment³

MyVA Workstream	MyVA Workstream Mission	My VA Workstream FY2015-2016 Goals	VA Strategic Objective Alignment
Veteran Experience	Supporting VA’s delivery of excellent care and benefit experiences that prioritize the perspectives and needs of our customers: Veterans, their families, supporters, and communities.	<ul style="list-style-type: none"> • Achieve Initial Operating Capability (IOC) for Veterans Experience team and Regional Veterans Experience offices • Create IOC for a front door, unified, digital experience for VA’s websites • Establish the Veteran’s identity and military service status at an enterprise level • Achieve IOC for collaboration through structured forums with community Veteran leaders • Establish a VA-wide customer satisfaction measurement • Design and begin implementation of the “To Be” Veteran experience • Develop a menu of services for customers to understand VA benefits and services for which they may be eligible 	<i>VA Strategic Objective 1.2:</i> Increase Customer Satisfaction through Improvements in Benefits and Services Delivery Policies, Procedures, and Interfaces
Employee Experience	Build a collaborative, inclusive and results-oriented culture that inspires trust in order to improve the Employee Experience	<ul style="list-style-type: none"> • Transform into a responsible, performance-oriented culture • Attract and retain high performing candidates • Plan career paths and development • Engage capable employees 	<i>VA Strategic Objective 3.1:</i> Make VA a Place People Want to Serve
Support Services Excellence	Optimize the organization, functions and activities of VA’s core support functions that focus on delivery of world class services to VA facilities and organizations that directly serve Veterans	<ul style="list-style-type: none"> • Complete analyses of existing VA support services • Design “future state” capabilities • Identify “quick wins” for focused execution efforts • Develop implementation plans for “future state” capabilities and begin execution • Track progress through measurements of “effectiveness” (e.g. improved customer satisfaction, faster time-to-market, etc.) and/or gained “efficiencies” (e.g. cost savings, reduced manpower requirements) 	<i>VA Strategic Objective 3.3:</i> Build a Flexible and Scalable Infrastructure through Improved Organizational Design and Enhanced Capital Planning

³ FY 2013-2015 Enterprise Roadmap Addendum. Department of Veterans Affairs. May 29, 2015.

<p>Performance Improvement</p>	<p>Partner across VA to support improvement efforts, while establishing an enterprise-wide Lean strategy and network that enables a culture of continuous process and outcome improvement</p>	<ul style="list-style-type: none"> • Outline milestones, goals, and Key Performance Indicators (KPI) • Develop & implement staffing plan Build communication and outreach plans • Establish Support Council and engage with critical partners • Adopt and tailor VERC KM Platform for enterprise access to KM resources • Launch two Districts • Support Council will evaluate the utility of Baldrige Criteria as an outcome measure 	<p><i>VA Strategic Objective 1.2:</i> Increase Customer Satisfaction through Improvements in Benefits and Services Delivery Policies, Procedures, and Interfaces</p>
<p>Strategic Partnerships</p>	<p>Leverage resources external to the VA on an effective and consistent basis, at all levels of the Department, to improve the Veteran experience while enhancing productivity and efficiency</p>	<ul style="list-style-type: none"> • Opportunistically match external offerings to help with emerging and external Veteran needs • Empower VA employees with the tools and support to engage in mutually beneficial partnerships at all levels of VA • Proactively solicit and engage in partnerships • Sustain, improve, and replicate established partnerships to more effectively leverage resources and serve Veterans • Conduct a feasibility study to build a VA Foundation to serve as a vehicle to engage in partnerships otherwise not possible 	<p><i>VA Strategic Objective 2.2:</i> Enhance VA’s Partnerships with Federal, State, Private Sector, Academic Affiliates, Veteran Service Organizations and Non-Profit Organizations</p>

1.1.2 Additional Business Drivers

In addition to MyVA, there are other business drivers that can impact VA infrastructure. Table 2 lists these business drivers and their implications for VA IT, including the level and time frame of their impact.

Table 2: Additional Business Drivers of VA Infrastructure

Driver	Implications	Impact	Time
Growth trends in Veteran population filing claims	Increase capacity for health- and benefits-related information exchange by increasing computation resources and automation	High	Near-Term
Shift towards customer-centric healthcare business model	Provide increasingly convenient and more integrated Veteran healthcare access: <ul style="list-style-type: none"> • Enable real-time information sharing to improve coordinating with external providers and monitor provided care • Offer mobile applications • Implement self-services, such as telehealth, telemedicine, VA Point of Service Kiosk, and next generation MyHealtheVet. 	High	Near-Term
	Build measurability into systems to improve business processes: <ul style="list-style-type: none"> • Increase use of Big Data Analytics to leverage data about quality, cost, access, and satisfaction 	Medium	Long-Term
	Expand productive and responsible public and private partnerships to more effectively serve Veterans: <ul style="list-style-type: none"> • Develop a culture of partnership that encourages collaboration • Align virtual technologies to establish unified IT delivery capability for Veterans and staff across all VA services and technologies. 	Medium	Long-Term
Federal and VA Policies	Health Insurance Portability and Accountability Act (HIPAA) laws: <ul style="list-style-type: none"> • Better accommodate Protected Health Information (PHI) requests, including sending data in requested forms and formats 	High	Near-Term
	Veteran’s Access, Choice, and Accountability Act (VACAA or The Veteran’s Choice Act): <ul style="list-style-type: none"> • Increase use of external providers • Resolve wait time and scheduling issues • Improve health record exchange services 	High	Near-Term
	Telework Enhancement Act: <ul style="list-style-type: none"> • Reduce costs of office spaces and traveling by employing telework 	Medium	Near-Term
Cost of IT	Ensure IT spending has clear return on investment and allocate overall resources efficiently	Low	Long-Term

1.1.3 Strategic Priorities

The VA OI&T mission is to “collaborate with our business partners to create the best experience for all Veterans.”⁴ OI&T is implementing various enterprise level initiatives to position VA to accomplish VA Strategic and Priority Goals that serve as the basis for transforming VA into a technologically modern organization. To meet mission success, VA’s Enterprise IT Transformation requires guidance by four key principles: transparency, accountability, innovation, and teamwork.

OI&T’s strategic framework for success is depicted in Figure 2. In order to enable long-term change, the framework must be agile and center on three key themes: stabilize and streamline core processes and platforms, eliminate material weaknesses, and institutionalize new sets of capabilities to drive improved outcomes.

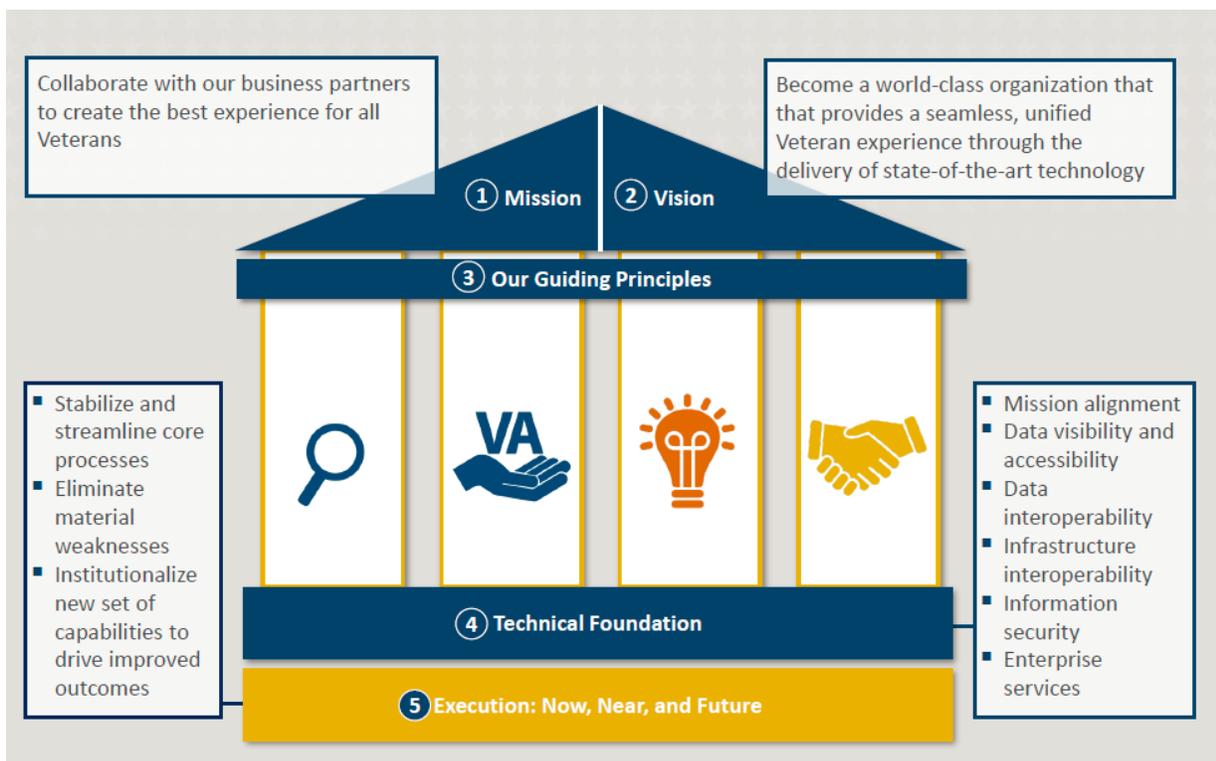


Figure 2: OI&T's Strategic Framework⁴

⁴ OI&T Enterprise Strategy Town Hall. Department of Veterans Affairs. October 21, 2015.

1.2 Current Environment

VA OI&T currently serves a complex IT infrastructure that supports approximately 325,000⁵ VA employees nationwide. These employees oversee and facilitate VA IT product and service delivery activities to over 21 million Veterans.⁶

IT is integrated across 152 Medical Centers, 300 Vet Centers, 820 Community-Based Outpatient Clinics, 135 VA Community Living Centers, 6 Independent Output Clinics, 104 Domiciliary Residential Rehabilitation Centers, 231 National and State Cemeteries, and 56 Regional Offices.⁵ VA owns and manages most of the infrastructure that it supports. Its vast technology profile includes over 424,000 desktop computers, 69,000 laptops, 31,000 mobile devices, and 539,000 email accounts.⁷ The VA technology environment consists of applications with a dedicated infrastructure and a project-centric IT service delivery model. It is based on delivering incremental customer-facing functionality every six months or less.

VA's distributed computing environments, in which components are shared among multiple computers to improve efficiency and performance, are characterized as tightly coupled systems. Coupling refers to the degree of direct knowledge that one component must have over another. Low coupling often indicates the design of a well-structured system, with reduced maintenance demands. It was determined that the VA's computing environment could benefit from an integrated design, an ability to reuse existing IT investments, and the application of industry standards.

The current IT environment, shown in Figure 3, depicts a set of layers of the core IT services and capabilities of the Enterprise Technical Architecture (ETA) Domains. The ETA is supported by policies and architecture products which are driven by a variety of key technology drivers. These key drivers allow for the interoperability of the VA IT environment.

⁵ 2014 Performance and Accountability Report. Department of Veterans Affairs. November 17, 2014. <http://www.va.gov/budget/docs/report/2014-VAparFullWeb.pdf>

⁶ Veterans Statistics – Veterans Day 2015. US Census. November 11, 2015. <http://www.census.gov/library/infographics/veterans-statistics.html>

⁷ Congressional Submission for FY2016 Funding and FY2017 Advanced Appropriations. Department of Veterans Affairs. <http://www.va.gov/budget/docs/summary/Fy2016-Volumell-MedicalProgramsAndInformationTechnology.pdf>

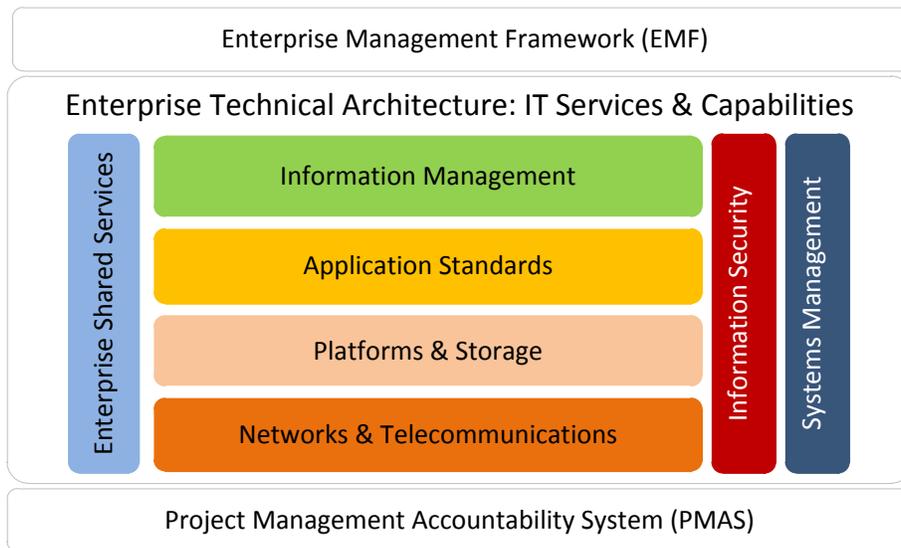


Figure 3: Current VA IT Environment

Although the current VA IT environment is characterized by infrastructure diversity, with an infusion of modern and legacy technologies, VA has made progress in the direction of its technology target state. Enterprise Design Patterns have been developed in the areas of Privacy and Security, Enterprise Architecture (EA), Interoperability and Data Sharing, IT Service Management (ITSM), Mobility, and Cloud Computing. These Enterprise Design Patterns act to guide solution architectures and ensure technical alignment between Business Product Management and Technical Platform Management solution architectures.

VA also continues to strengthen cyber security capabilities through the Continuous Readiness in Information Security Program (CRISP). In addition, the Ruthless Reduction Task Force (RRTF) optimizes VA’s application environment to reduce redundancies, while integrating systems and capabilities. Efforts such as these create a foundation for VA to transform the technology environment by applying industry standards and incorporating integrated design and reusable IT investments.

1.3 IT Services and Capabilities

VA OI&T provides the full range of IT equipment, services, solutions, and customer support to meet the VA mission and its business requirements. VA employees rely on IT services in their daily use of computers, mobile devices, e-mail, Intranet, and mission-critical software applications. Table 3 depicts a high-level overview of OI&T services and capabilities.

Table 3: OI&T Services and Capabilities

Service	Capability
Application Standards	Specification, design, construction, implementation, and lifecycle management of software applications, including application layer communication, presentation, and business logic services
Information Management	Organized storage, retrieval, management, and analysis of collected data
Platforms & Storage	Hardware and software platform delivery, which support computing applications and data storage
Networks & Telecommunications	Standards, software, and hardware for computer networking and telecommunications
Systems Management	Management and administration of VA’s IT enterprise and associated facilities, assets, programs, and projects
Information Security	Information security (protecting data), computer security (protecting systems), and information assurance (people, products, and procedures to ensure data confidentiality, integrity, availability, assured delivery, and non-repudiation)
Enterprise Shared Services	Enterprise systems integration and information exchange

TS identifies candidates for future Enterprise Design Patterns and categorizes them by OI&T capabilities and services. The Enterprise Design Patterns represent the key elements of the VA ETA. Project teams use them to achieve standardized solutions and approved technologies from the Technical Reference Model (TRM). The Enterprise Design Patterns support the individual capabilities or a combination of them. The capabilities, in turn, align to ESS architecture by ASD Product Engineering. IT investment planning for each technology category is located in the TRM.

2 ANALYSIS OF CURRENT ENVIRONMENT

An increase in the volume of electronic transactions, such as digital claims, electronic medical records, and telehealth data, has accelerated the demand for infrastructure capacity and reliability. The current IT infrastructure includes poorly integrated systems, duplicative platforms, inefficient processes, capacity-demand mismatches, and excessive costs associated with the operation and maintenance of existing platforms.

As a result of evolving business and mission requirements, aging infrastructure and applications appear to be nearing the end of their capability to support the increasing demand placed on them. Aging systems may soon be unable to adapt to the demands for increased functionality, ubiquitous access, and increased security. VA will need refreshed and updated technology in order to be able to keep pace with the demand for services.

In addressing these challenges, OI&T performed environmental scans and identified gaps, drivers, and trends that shape the future state of IT infrastructure. Many factors influenced how VA employs infrastructure, including emerging technologies and regulations. VA needs to be flexible enough to appropriately react to internal and external influences.

3 TRANSITION ACTIVITIES TO ADDRESS INFRASTRUCTURE GAPS

3.1 Infrastructure Gaps

The infrastructure gap assessment is based upon the review and analysis of actual performance, as compared to the desired or potential performance that is necessary to achieve the VA future state. The gaps were identified by evaluating the issues in each area as compared to the “To Be” vision. The gaps are depicted in Table 4.

Table 4: Infrastructure Gaps and Future State for each Capability

Current Gap	Description	IT Vision Future State
Cloud Computing & Infrastructure	VA has invested in cloud computing at the project level, resulting in regional capabilities without adequate governance and policies.	Technologies that provide elasticity, scalability, economies of scale, rapid deployment, and capacity sharing.
Security	Access to many domain specific capabilities, such as unique databases, requires multiple sign-ons. This leads to security issues as users sign on and off multiple times, as well as other issues, such as network boundaries, mobile technology, and data centers.	Protect information in the network and during handoff to external partners. Authenticate devices, processes, and people at appropriate points in accordance with an Enterprise Cybersecurity Strategy.
Information Management	There are multiple independently-updated databases containing the same data elements, and sometimes different or outdated values record. Without an Authoritative Data Sources (ADS), Veterans, employees, and partners lack the availability of robust information on demand. This duplicative or inconsistent data incurs extra management costs and lacks the efficient delivery of information and services to Veterans.	Shared enterprise data approaches that enable data analytics, data sharing, and management across many infrastructure platforms.
Interoperability	Applications under development do not have shared services available causing non-standard user interfaces, data exchanges, performance monitoring, and security implications.	Enterprise applications and external partner systems shared services to exchange, process and present information.
Mobile	Domain specific infrastructures, standards, data, and application interfaces limit a mobile enterprise environment.	VA staff and Veterans can use any approved device that may or may not be hardwired into VA's network, to access government information anytime, anywhere.
Application Modernization	VA's distributed computing environments are characterized as tightly coupled systems that would benefit from integrated design, ability to reuse existing IT investments, and industry standards.	Enterprise applications are built as dynamic websites that adapt, and mixed with the most suitable Commercial-off-the-Shelf (COTS) and or Government-off-the-Shelf (GOTS) solutions.
Collaboration	There is a need for centralized, enterprise-grade collaboration services for IT governance, content, and records management and enterprise portals.	Provide centralized collaboration services for disseminating information and integrated user interfaces for accessing services.

The ETSP will guide decisions regarding IT services, processes, applications, systems, technologies, resources, security, risk, and timeliness to address these gaps and improve the infrastructure environment. OI&T invests in faster, more agile methods to develop products and services that help support the cost-effective and secure delivery of health care and benefits to Veterans. For example, as the healthcare industry and VA business functions change, OI&T will need to continue to improve and invest in enhanced cyber security policies, standards, and technologies. Identified OI&T actions include the development of a Cyber Security Solution to

secure Veteran data within the next five years and the development of a resilient Cyber Security Architecture to support a robust, customer-centric mobile application framework.

OI&T also identified the completion of the implementation of Personal Identity Verification (PIV)-only authentication as a key step towards improving the VA environment. In order to effectively deliver health care and benefit services, VA personnel require access to a single, holistic view of Veteran data stored in VA trusted partner systems and increased access to self-service capabilities. Thus, VA applications should be designed for use on any type of device (e.g., mobile, desktop).

OI&T requires a unified approach to designing, engineering, and delivering IT solutions, with an underlying goal of eliminating the development of duplicative capabilities and functionality. Enterprise Design Patterns provide standardized guidance to VA project teams on how to leverage each OI&T capability and service, in accordance with enterprise IT governance policies.

Table 5 shows transition activities that are necessary to bridge the current infrastructure gaps and how they align to currently published Enterprise Design Patterns.

Table 5: Transition Activities and Enterprise Design Patterns Alignment

Current Gap	Related Enterprise Design Patterns	Transition Activities	Implementation
Cloud Computing & Infrastructure	IT Service Management	Standardize IT Platforms	Long-term
	Cloud Computing	Cloud Computing	In progress
Security	Privacy and Security Enterprise Architecture IT Service Management	Continuous Readiness in Information Security Program	In progress
		Predictive Scanning Portal Pilot	In progress
		Privacy Training	In progress
		Privacy Awareness	In progress
		Data Validation	In progress
		Privacy Impact Assessments (PIA) Automation Tool	In progress
		Trusted Internet Connection	In progress
		Homeland Security Presidential Directive	In progress
		Continuous Monitoring	In progress
		Veterans Health Information Systems and Technology Architecture (VistA) Evolution	Near-term
Information	Enterprise Architecture	Manage Data as an Asset	Mid-term

Management	Interoperability and Data Sharing	Veteran Benefits Management System	In progress
Interoperability	Enterprise Architecture	Enterprise Shared Services	In progress
	Interoperability and Data Sharing Mobile Architecture	VistA Evolution	Near-term
Mobile	Mobile Architecture	Mobility	In progress
		Mobile Device Management	Near-term
Application Modernization	Enterprise Architecture	Open Source	In progress
	Interoperability and Data Sharing Mobile Architecture	VistA Evolution	In progress
Collaboration	Enterprise Architecture Interoperability and Data Sharing	National Service Desk	In progress
		IP Video to Home National Expansion	In progress
		Next Generation Satellite Communications	In progress

4 FUTURE ENVIRONMENT

4.1 VA IT Vision

The IT vision is achieved through a robust, secure, agile, and interoperable infrastructure. The VA IT security controls will be executed in alignment with the VA Handbook 6500.⁸ Ultimately, these actions will lead to more cost effective investments in usable interface design that provide opportunities for service and benefits delivery that currently do not exist. Figure 4 depicts the VA 5-year IT vision and illustrates how new technologies can provide an environment that effectively support mission attributes. Appendix A introduces the VA IT Vision (3-year) to achieve an interim state.

⁸ VA Handbook 6500. Department of Veterans' Affairs. March 2015.
http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=793&FType=2

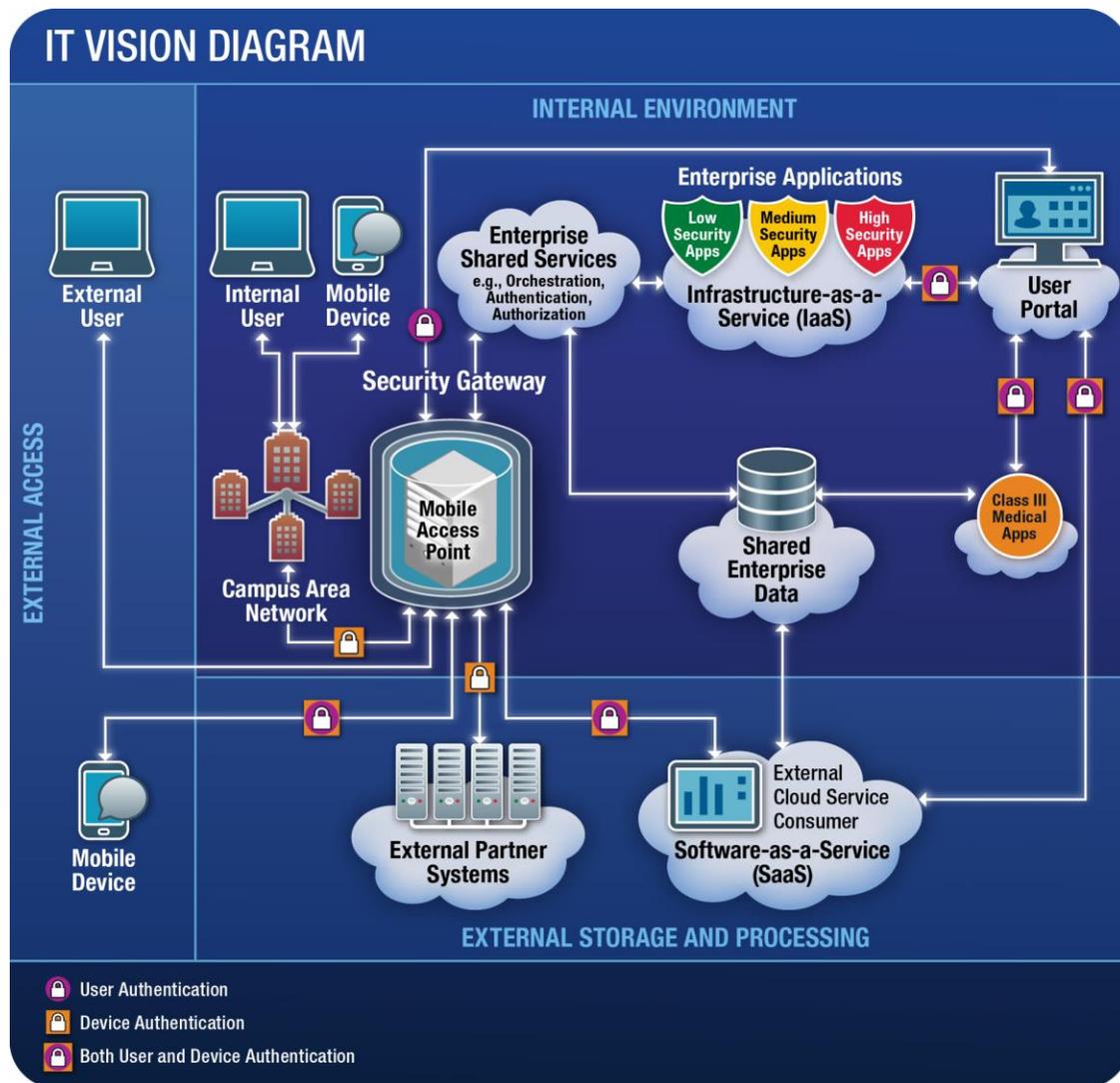


Figure 4: VA IT Vision Diagram

4.1.1 Internal Access

An Internal User is any VA employee with VA issued access credentials. An Internal User will access enterprise resources through a robust networking infrastructure via the Campus Area Network, where the Internal User device will be authenticated. VA policies require the use of PIV cards for internal user authentication to VA resources, or other two factor authentications to protect privileged access to data, applications, and networks.

The Internal User will also be able to access enterprise resources via a Mobile Device. VA facilities nationwide will be connected to VA's network infrastructure. User identity is authenticated through a Security Gateway, containing a Mobile Access Point, which routes an authentication request to ESS for identity management. After the Internal User is authenticated, the Internal User can use the User Portal to access applications that are

provided on a cloud computing platform, as an Infrastructure-as-a-Service (IaaS); and applications hosted on multiple platforms, as Software-as-a-Service (SaaS) clouds. External applications that are hosted in an off-premises cloud environment will be fully integrated with the enterprise IT infrastructure; they will be monitored as an on-premise hosted application. VA internal and external users will access data and services by means of a SSO functionality. The Federated identity management (FIM) system, an arrangement that lets subscribers use the same identification data to obtain access to the networks of all enterprises in a group of multiple enterprises, is transitioning VA to an Identity and Access Management (IAM) SSO, known as AccessVA. AccessVA is a single-entry-point online where Veterans, beneficiaries, and affiliates log on and are provided with access to multiple government websites and applications. It will allow users to log in once with existing credentials to access their services and facilitate sharing identity information across administrative boundaries. User credentials will be passed along as they traverse the VA infrastructure. The credentials will allow role-based access to services and data authorized for each user.

4.1.2 External Access

An External user is defined as any user accessing a public facing site over the Internet. External users will also be able to access enterprise resources by means of a Secure Gateway and Enterprise Shared Services, after user authentication access level permissions to enterprise data have been determined. In this case, the user device will not be authenticated, since the External User can choose to use any device to access the portal. External partner systems will also be able to access a wide range of enterprise resources via a system-to-system exchange.

External Users will be able to access enterprise resources on a mobile device by means of a Mobile Access Point within the Security Gateway. VA Internal and External Users will access services and data by way of a SSO functionality. VA has adopted a federated approach that allows the use of many different credential types to access VA resources. This approach allows external users to authenticate to requested VA information resources using the credential that is most convenient for them, given that it meets the proper level of authority (LOA). The goal is to provide users with access to multiple VA resources without requiring separate authentication for each one. This approach achieves the goal of increasing access to VA resources while eliminating complexity for external users.

VA has approved a number of external Cloud Service Providers (CSPs) in order to support a variety of credentials and LOAs and will continue the process of approving CSPs as needed. It is expected that the creation of the Federal Cloud Credential Exchange (FCCX) would allow VA to leverage CSPs and may reduce or eliminate the need for VA to separately approve CSPs on a case-by-case basis.

4.1.3 Applications

There are three different enterprise applications that are used to represent different types of access. The lowest level of authorization required is the green Low Security Applications. The

Low Security Applications have access control policies that require a low level of authorization that do not have strict role-based requirements on who can access data.

The yellow Medium Security Applications align to specific roles. Thus, they make the data available only to the roles that permit visibility of that data.

The highest level of authorization required is the red High Security Applications. The High Security Applications control sensitive information, such as Personally Identifiable Information (PII) or Protected Health Information (PHI), and manage the authorization to access that information.

While data in the red High Security Applications is at rest, or not moving through the network, the data will be encrypted. This is a requirement for applications that use Government data; the encryption must follow Federal Information Processing Standard 140-2 standards. The (Mobility) Mobile Architecture V2.0 Enterprise Design Pattern⁹ provides architectural guidance on encrypted data at rest for mobile devices. The industry standard and future direction is to use full disk encryption (FDE) for VA data at rest or in transit. FDE is the encryption of all data on a disk drive. It functions by automatically converting data on a hard drive into a form that cannot be understood by anyone who does not have the key to undo the conversion.

Class III Medical Applications are used for medical devices within VA facilities to call on services. These applications are subject to Food and Drug Administration (FDA) regulations and VA asset management policies. They depend upon other ESS to provide business rules that define specific types of sensitive information that have role-based access.

4.1.4 Device and User Authentication

In most instances, users will be authenticated and device integrity will be verified to minimize security issues. Device authentication protects data using enterprise capabilities, giving software authentic information about what sort of hardware it is communicating with. User authentication confirms the identity of individuals accessing the enterprise resources.

The future technical state will include attribute management services for conducting enterprise-wide Attribute-Based Access Control (ABAC), using current and emerging open standards. ABAC is a paradigm in which access rights are granted to users through the use of policies which combine attributes together. Centralized enterprise auditing services will be deployed to log service calls, including calls for PII and PHI. These services will track data access activities and exception handling, leading to an increased security posture for VA's enterprise resources.

⁹ (Mobility) Mobile Architecture V2.0 Enterprise Design Pattern. Department of Veteran's Affairs. http://www.techstrategies.oit.va.gov/docs_design_patterns.asp

4.1.5 Enterprise Shared Services and Data

Applications will integrate with ESS to gain virtual access to Shared Enterprise Data through the use of a common set of Data Access Services (DAS). DAS will include an extensible Enterprise Create, Read, Update, Delete (eCRUD) service, for which advanced management and functionality of the data will operate for both in-house or commercial-off-the-shelf (COTS) applications. These applications include open-source, to gain access to Authoritative Data Sources (ADS) by the use of an Application Programming Interface (API) that adheres to open standards (e.g., Representational State Transfer). These APIs will provide a level of abstraction since that they do not need to know the specific details of the service implementation, and they do not require physical access to databases in order to obtain data.

ESS will also provide enterprise capabilities for data aggregation to bring together output from multiple data sources in a summary form. This ensures semantic harmonization, user authentication services, and the arrangement of diverse services to support the automation of business processes and workflow across the enterprise.

The Enterprise Design Patterns include ESS and IAM traceability. The Enterprise Design Patterns have been used by projects primarily as guidance to integrate with ESS and IAM, and to migrate existing functionality to the ESS environment. Projects are required to provide ESS and IAM integration in System Design Documents that are reviewed by Architecture and Engineering Review Board (AERB).

4.1.6 Attributes of Future IT Environment

VA's IT target state describes an environment that utilizes a variety of new and emerging technologies. When combined, the emerging technologies constitute a dramatic shift in the way VA capabilities and services are acquired and provisioned; how applications are designed and implemented; how information is accessed, exchanged, processed and retained; and how data and the IT infrastructure are protected.

The attributes of the future environment, as shown in Table 6, include information availability, information security, reusable shared services, modern applications, and scalable infrastructure. These attributes will allow VA staff and Veterans to securely connect a multitude of devices to the VA network, with ubiquitous access from any location at any time. Devices, processes, and people will be authenticated at appropriate points as they move between functions and require different levels of authorization. VA will utilize technologies, including cloud technologies, that provide elasticity, scalability, and shared capacity.

Table 6: Attributes of Future Environment

Attribute	Description
Easily Accessible Information	VA shall leverage technologies that allow VA staff and Veterans to access information via a multitude of devices that may or may not be hardwired into VA’s network from any location and at any time.
Secure Information and Networks	Information shall be protected through encryption as it traverses through the network. Devices, processes and people will be authenticated at appropriate points as they move between functions requiring different levels of authorization.
Reusable Shared Services	Enterprise applications and external partner systems shall use ESS to exchange, process and present information to improve interoperability, reduce system development costs and accelerate delivery.
Modern Applications	Enterprise applications shall be built as dynamic websites that adapt to how various browsers need to translate and display information. VA adopts the most suitable COTS and GOTS solutions.
Scalable Infrastructure	VA shall leverage technologies that provide elasticity, scalability, and cloud technologies that allow the sharing of capacity, support mobility, data analytics, and shared authoritative data.

To realize the IT vision, VA IT investments must align with the VA Enterprise Architecture (VA EA) through incremental change and alignment with VA policies and existing architectures. These include the VA Strategic Plan, MyVA business drivers, Enterprise Target Application Architecture, OI&T Infrastructure Architecture, TRM, and Information Security Architecture.

4.2 Transition Activities for Cloud Computing & Infrastructure Gaps

The manner in which VA acquires, installs, and manages networks is currently limited. VA is undertaking several cloud and infrastructure initiatives to address these gaps.

4.2.1 Infrastructure Optimization

Implementing and maintaining an efficient IT environment and utilizing an agile, reusable, and modernized infrastructure is key to optimizing the IT services at VA. Leveraging new technologies and best practices promotes innovation and allows an enterprise to transition from existing Capital Expenses (CapEx), such as outdated hardware, to more Operational Expenses (OpEx), such as cloud computing and internet communications. This allows an enterprise to reduce investment and maintenance costs, while modernizing infrastructure.

VA IT Infrastructure Modernization is driven by changes in philosophy and budget. VA is currently evaluating needs to own and manage networks and devices, while still protecting the information that traverses the infrastructure. These modernization efforts are guided by on-demand capacity that is achieved by virtual environments, elasticity, and scalability. Key transitional activities related to optimizing the infrastructure include:

- Develop and execute a unified communication and collaboration strategy that enables a converged platform serving communications media (e.g., voice, data, video, chat, presence, and unified messaging).
- Consolidate 300 VA data centers as a long-term initiative under the Federal Data Center Consolidation Initiative (FDCCI), an Executive branch mandate requiring government agencies to reduce the overall energy and real estate footprint of data centers, with the targeted goals of reduced costs, increased security, and improved efficiency.
- Implement a Digital Operating Environment that supports paperless administration of Veteran benefits.
- Continue to implement the Enterprise Management Framework (EMF), which will support a unified enterprise service management model that includes release management, configuration management, change management, and incident management.
- Develop a roadmap from the current de-centralized framework to the more versatile and flexible centralized network framework, utilizing Software Defined Networking (SDN) and generic, non-proprietary, hardware and software.
- Develop a total Platform-as-a-Service (PaaS) cloud broker solution that automates the deployment of Enterprise Design Patterns, solution environments, and supports business specific code to any infrastructure.

There are several opportunities in the VA environment to leverage SDN. Use cases for SDN include:

- Latency sensitive mission applications, intelligently and automatically re-routed around network congestion
- Dynamic provisioning of network resources for an internal cloud
- True on-demand infrastructure

The latest culture of cyber-terrorism, hacking, and zero-day vulnerabilities creates a formidable challenge for any large organization, and VA is no exception. SDN promises an opportunity to automate detection and neutralization of a threat or information security incident.

While VA could benefit from SDN, it is not supportable with VA's current network infrastructure. Manufacturers of network hardware continue to make progress developing SDN technologies for existing install bases. Having a network infrastructure capable of SDN is a necessary first step. However, further defining and refining the use cases, developing the SDN programmatic interfaces to the infrastructure, and building the "network intelligence" is currently a requirement. VA has taken initial steps towards developing a roadmap from the current de-centralized network framework to the more versatile and flexible centralized network framework; that is the essence of SDN.

4.2.2 Cloud Computing

Cloud Computing is the networking of large groups of servers to allow online centralized data storage and access to computer resources or services, rather than on a local server or a personal computer. Also known as on-demand computing, cloud computing enables organizations to consume resources like a utility, much like electricity, rather than building infrastructure in-house. Cloud Computing is the enabler that allows enterprise IT infrastructure to provide agile services, such as shared services, mobile accessibility, and information management. In addition to the agility, accessibility, and capabilities that cloud computing offers, the switch from a depreciative CapEx to a renewable OpEx will cut costs. Information security risks are minimized when applications, operating systems, and data reside in an appropriately secured cloud environment, rather than on a device; the threat to VA data assets will be limited in the event a device is lost, stolen, or compromised.

Adopting a utility cloud computing model for server environments provides agile, scalable, and reliable infrastructure that is needed to keep pace with the explosive growth of information and information assets. An example of this began during FY12, when OI&T started offering IaaS 92 at the Austin Information Technology Center (AITC). The project included support for on-demand, self-service provisioning; broad network access; resource pooling; rapid elasticity; and measured service.¹⁰

VA OI&T continues to pursue Cloud Computing initiatives that pave the way to increase capacity and capabilities, without investing in new infrastructure, training new personnel, or licensing new software. Users can commission or decommission virtual environments with minimal service provider interaction. Key transition activities related to delivering cloud capabilities include:

- Identifying, consolidating, and integrating operational VA data stores to facilitate virtualization and location independence¹¹
- Expanding internal IaaS and PaaS offerings, such as the Enterprise Development Environment (EDE) that is located at the AITC and a hosting facility at Terremark in Culpeper, VA; near-term strategy involves deploying private cloud services and using public cloud services
- Continuing investigation of the viability of using external SaaS providers to deliver Email-as-a-Service, as compared to internally hosted options; SaaS includes specific capabilities beyond Email-as-a-Service that are hosted externally
- Implementing a cloud broker to aggregate, integrate, and customize internal and external cloud services

¹⁰ FY 2013-2015 Enterprise Roadmap, Department of Veterans Affairs. March 28, 2014.

http://www.ea.oit.va.gov/docs/VA_Enterprise_Roadmap_2_FINAL_20140409.pdf

¹¹ (Interoperability and Data Sharing) Hybrid Data Access Enterprise Design Pattern. December 28, 2015.

VA is defining an enterprise cloud strategy that aligns with leadership vision, considers policy constraints, and delivers value to IT architecture design patterns. In April 2015, the Office of Service Delivery & Engineering (SDE), ASD, and Office of Information Security (OIS) directed development and definition of VA's cloud computing strategy. As a result, a new Decision Document is being finalized to describe the agreed upon changes to VA Directive 6517. The specific changes include:

- Reflection of roles and responsibilities of a VA Cloud Services Broker.
- Addition of Cloud Consumer management responsibilities.
- Alignment of roles with specific VA organizations.

A cloud broker is an entity that manages the use, performance, and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers. OI&T leadership agreed that the Cloud Broker function is a shared responsibility of ASD (business) and SDE (technical).

SDE will serve as the VA Technical Cloud Broker, an entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.

ASD is responsible for implementation standards for IT solutions that best serve Veterans. ASD enforces Veteran-serving IT solutions standards, while exercising proper stewardship of resources and maintaining transparent operations.

A cloud consumer represents a person or organization who receives services and maintains a business relationship with a cloud provider. Internal VA cloud consumers will be represented by a single central cloud consumer resident in the Office of Product Development (PD). PD will have three key responsibilities in this role: develop and maintain the Enterprise Cloud Service Catalogue; coordinate the technical cloud broker to lead Technical Working Groups to standardize Service Deployment across the OI&T Pillars; and provide the Authority to Operate and ensure that process standards, Plans of Action, and Milestones requirements are met.

The Technology Acquisition Center (TAC) in the Office of Acquisitions Operations, under the Deputy Secretary for Acquisitions and Logistics, is part of the contracting, acquisition and procurement staff for VA. To advance the facilitation of cloud computing, the TAC will work closely with the business and technical cloud broker and the central cloud consumer, providing acquisition and contracting support.

4.2.3 IT Platforms Standardization

A key step for VA to consolidate IT infrastructure is to standardize IT platforms and streamline system deployment across multiple business units. Standardizing platforms serves to minimize

program-unique infrastructure. A standard platform design ensures a secure cyber environment, reduced cost, increased agility, flexibility, and interoperability. Key transition activities related to standardizing the platforms include:

- Identify, develop, and mandate the use of enterprise-wide shared IT platforms.
- Establish a single interface to the Veteran with a portal platform and mobile application delivery platform(s).
- Sustain a National Service Desk (NSD) to stay in alignment with user and service levels and implement usage of NSD by programs.
- Include open source tools and applications in the TRM.
- Continue standardizing and consolidating development and test environments through preproduction.
- Continue standardizing end user device operating systems.
- Select and support commoditized hardware products to become available via the Commodity Enterprise Contract, which includes commodity hardware products such as laptops, mobile tablets, thin clients, servers, switches, routers, firewalls, and storage, based upon infrastructure standards published in the VA EA and TRM.

4.2.4 National Wireless Infrastructure

The National Wireless Infrastructure Project provides a wireless, location-based infrastructure across VA facilities, using standard technologies and protocols throughout the enterprise. The new solution provides encryption and security for access points and clients, and is designed to meet any future VA IT requirements. It supports critical functions such as Bar Code Positive Patient Identification for the safe administration of medications and planned capabilities, including Real Time Location Services for improved asset management.

In FY13, OI&T installed wireless capability at 16 VA Medical Centers (VAMCs), bringing the total number of completed installations to 81 sites.¹² Additionally, requirements were finalized and acquisitions were completed to support the deployment of wireless to an additional 61 VAMCs in FY14 and the remaining 35 sites in FY15.¹³

4.3 Transition Activities to Address Security Gap

VA's current security approach requires network access servers and application access devices to be managed with a single authentication service, with a dependence on MS Active Directory

¹² Homeland Security Presidential Directive (HSPD) 12. Department of Agriculture. June 2, 2015. <https://hspd12.usda.gov/about.html>

¹³ CIO Annual Report. Department of Veterans Affairs. 2013 (Draft).

for authentication. This authentication method requires multiple sign-ons for domain specific capabilities, which leads to security issues, as users sign on and off multiple times. VA is undertaking several related initiatives to address the gaps in security.

VA uses tightly coupled systems that are designed for specific uses, but which result in duplicative information management and systems. By decoupling information from the presentation and converting it to an open data format, data is reusable. Decoupling also allows security controls to be embedded into data and metadata directly, rather than through a device.

VA's secure target state is predicated upon implementing an integrated, comprehensive threat-based security architecture. This architecture includes data privacy and securing VA's sensitive information, systems, software, and networks from breach and intrusion.

The OIS operations mission statement explains that, "OIS is devoted to supporting all stages of Veteran care by protecting the personal information of Veterans and the employees who serve them."¹⁴

- OIS, within OI&T, has full responsibility for VA's information security and privacy programs.
- OIS provides services, tools, guidance, oversight, and direction to VA Administrations and staff offices.

VA is working to ensure that IT investments support the IT Vision goals to provide continual improvements in information security and privacy. VA has established numerous cybersecurity and privacy measures to support the President's cross-agency goals of continuous monitoring, Trusted Internet Connections (TICs), Homeland Security Presidential Directive 12 (HSPD-12) implementation, and safeguarding the Department's holdings of PII and sensitive but unclassified information.

Cybersecurity investment ensures VA investments, programs, and initiatives align with and take full advantage of VA's cybersecurity capabilities. The ESS working group leads ongoing development of an overarching Security Architecture program that will encompass all layers of the VA enterprise. This Security Architecture program will be capable of delivering and maintaining desired cybersecurity attributes, including confidentiality, integrity, availability, accountability, and assurance that is consistent with a "defense in depth" approach.

The ESS working group is currently focused on VistA Access enhancements and developing the new Secure Token Service (STS). These programs are working to resolve the Non-Personal Entry

¹⁴ Office of Information Security (OIS) Overview. Department of Veterans Affairs.
http://www.ois.oit.va.gov/OIS_Overview.asp

issues throughout the VA, as defined in the (Privacy and Security) Non Person Entity Authentication Enterprise Design Pattern. A pilot program is currently underway to test the STS solution.

Alignment and compliance with VA cybersecurity rules and standards are established and maintained through architecture compliance and security assessment and authorization. VA rules and standards ensure compliance with federal information security and privacy legislation. Adherence is evaluated and verified at each project management process development milestone.

VA IT capabilities are required in order to receive full security assessment and authorization prior to IOC deployment, as part of the project management process development. Once deployed, VA IT capabilities are continuously monitored throughout the lifecycle using enterprise-wide security enhancements. This activity is part of the maintenance of the Department's infrastructure capabilities.

OIS integrates privacy throughout the lifecycle of each system by aligning with the Federal Information Security Management Act (FISMA). VA complies with privacy compliance requirements by conducting Privacy Threshold Analysis (PTA), Privacy Impact Assessments (PIA), and documenting Systems of Record Notice (SORN) in the Federal Register. OIS establishes and maintains an inventory of programs and information systems identified as collecting, using, maintaining, or sharing PII.

OIS developed a strategic budget implementation plan to guide and prioritize investments in emerging cybersecurity capabilities. Systematic evaluations and impact rankings compared to OIS defined goals and objectives are used to decide the investment and portfolio decisions. This analysis ensures VA compliance with federal information security standards, federal privacy protection laws and regulations, standard security controls, and VA directives. This robust information security and privacy system supports the Chief Information Officer's (CIO) strategic priority, regarding Next Generation Information Security and Privacy, as well as OI&T Objective 2.3.

4.3.1 Continuous Monitoring

The OIS continuous monitoring program completed the first two phases of the Visibility to Everything (V2E) project. Critical data delivered by the V2E project has significantly increased the visibility of devices, servers, voice and video devices, layer 2/3 network interfaces, wireless Local Area Network controllers, firewalls, routers, switches, and Wide Area Network traffic optimizers.

The project addressed vulnerabilities discovered on over 453,000 machines.¹⁵ Extensive near-real-time reports and cybersecurity analysis generate executive dashboard summaries that report requests to meet customer requirements and artifacts. These provide program reviews, analysis, and recommendations to remediate and re-architect initiatives to the existing VA Security Architecture. The Veterans Health Administration (VHA) Biomedical Engineers use the same network for monitoring the Medical Device Information Architecture.

4.3.2 Homeland Security Presidential Directive

OI&T implemented middleware that integrates the HSPD-12 PIV system, the VA Public Key Infrastructure, and VA's Active Directory with local Physical Access Control Systems (PACS). The system provides digital identity and credentialing information from VA's HSPD-12 PIV system to connected PACS. This establishes a centralized data connection that provides data consistency, reuse of information, centralized reporting, holistic dashboard views, and a centralized approach to provisioning and de-provisioning access across disparate PACS within VA. During FY13, and the first quarter of FY14, the PIV PACS project successfully completed two increments.

VA has enabled the majority of user devices with Smartcard capabilities, and has issued PIV cards to 97%¹⁶ of employees and contractors. Currently, VA employees and contractors that work at the VA Central Office (VACO) campus are required to log into the VA network using a PIV card, while on campus. Plans are in place to require PIV card-based logical access throughout the enterprise.

4.3.3 Trusted Internet Connection/Einstein¹⁷

National Cybersecurity Protection System 2.0 (NCPS; formerly known as Einstein) devices are deployed in four VA TIC Gateways. VA remains committed to the implementation of critical requirements. VA is approved to operate as a TIC Access Provider for VA's four Internet gateways (Sterling, Virginia; Dallas, Texas; Chicago, Illinois; and San Jose, California) and meets federal requirements for TIC service providers. The TIC gateways continue to improve the security of the VA enterprise network by instituting common security controls and configurations and installing additional monitoring capabilities.

4.3.4 Information Security

VA systems are compliant with VA Handbook 6500 and National Institute of Standards and Technology (NIST), as well as with additional VA-specific security controls. Other measures to ensure appropriate account management include automated mechanisms to audit account

¹⁵ VA Dashboard. Department of Veterans Affairs. <http://dashboard.tic.va.gov/s/ST/>

¹⁶ 2014 Performance and Accountability Report. Department of Veterans Affairs. November 17, 2014. <http://www.va.gov/budget/docs/report/2014-VAParFullWeb.pdf>

¹⁷ FY 2013-15 Information Resource Management Strategic Plan. Department of Veterans Affairs. March 28, 2014. http://www.ea.oit.va.gov/EAOIT/docs/VA_IRM_Strategic_Plan_Final_Signed_20140424.pdf

creation; modification, disabling and termination actions; and appropriate notification, as required.

4.3.5 Data Validation

The Data Validation project allows Privacy Service to gather disparate sources of data that impact privacy, such as PIA, PTA, SORN, forms, etc. The project also generates reports that provide information to improve privacy awareness within VA. It provides a gap analysis for business processes and management decisions.

Data Validation references the SORN. VA systems undergo a privacy assessment, which involves PIA and PTA. The SORN requirement is driven by the Privacy Act of 1974 and is generally required when any collection of PII exists and is accessed through a personal identifier. In general, a SORN is required if a system uses PII in a way that retrieves that information by personal identifier.

4.3.6 Privacy Impact Assessments Automation Tool

The PIA Automation Tool is a web-based interface that enables VA Privacy Service to manage privacy requirements of the e-Government Act. The tool allows users, such as IT system owners, Information Security Officers, and Privacy Officers, to create, edit and retain privacy related documentation (i.e., PIA and PTA for system inventory) in a Structured Query Language (SQL) database. As required by law, Privacy Service analysts administer the tool, review and approve the PIA and PTA submissions, and automatically publish the approved PIA to the Internet.

As required by OMB Memorandum 07-16, data in the automation tool is also used in the Data Validation project for purposes of analyzing and reducing PII holdings and Social Security Number usage and collection.

4.3.7 Privacy Training

VA Privacy Service is developing a standardized training curriculum for Privacy Officer Professionalization Training (POPT) to provide a baseline set of knowledge, skills, and abilities. The POPT program will offer seven web-based training modules and comprehension tests within the Talent Management System.

4.3.8 Privacy Awareness

VA Privacy Service launched an 18 month Privacy Awareness campaign that was designed to align with the Secretary's strategic plan. The internal campaign focuses on the topic, "Why should Veterans trust us? - Privacy Builds Trust." The goal is to rebuild trust internally by educating employees about privacy. The external campaign focuses on "Why Should You Trust Us? - Privacy Matters." This is an opportunity to reassure Veterans that the sensitive information they provide to VA remains confidential, secure, and protected.

4.3.9 Predictive Scanning Portal Pilot

Network and Security Operations Center (NSOC) Predictive Scanning Portal Pilot was launched to assist facilities in addressing vulnerabilities within scan results. NSOC developed a scan portal for regions and business units to log-in to update Internet Protocol (IP) address ranges prior to the monthly scan. Predictive scanning ensures vulnerabilities are remediated in a consistent manner and on a timely basis, and provides another tool to safeguard Veterans' sensitive data. The first pilot site in September 2013, conducted predictive scanning using the NSOC portal.

4.3.10 Continuous Readiness in Information Security Program

In support of VA's efforts to ensure protection of sensitive information, OI&T implemented CRISP, which provides cyber oversight of Veteran information. As a result, data breaches now abide by clear, documented contingency plans, and VA employees, contractors, and affiliates complete online security training.

CRISP promotes the theme that securing information is everyone's responsibility. Consistent CRISP security and privacy awareness training ensures that personnel who access VA information systems, data, or information, will improve VA's security posture.

Active management of software on VA's network ensures that only authorized software is installed, and unauthorized and unmanaged software is found and prevented from installation or execution. VA is developing an end-to-end process to identify unauthorized software found in the enterprise through discovery, data normalization, and analysis against the TRM. This process enables line-of-business organizations to make determinations about the necessity, criticality, regulatory controls, patient safety, and other operational limitations that dictate whether or not the software can be removed, updated, or scanned without endangering patient safety, violating federal regulations, or harming other critical operations.

In summary, CRISP efforts will:

- Result in implementation of processes that ensure VA organizations are included in the vulnerability management program and implement improved mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and Web application servers; and
- Develop a comprehensive list of approved and unapproved software, and implement a process for monitoring, preventing installation, and removing unauthorized application software on agency devices.

4.3.11 Veterans Health Information Systems and Technology Architecture

The Veterans Health Information Systems and Technology Architecture (VistA) is the VA's electronic health record (EHR) system. VistA is designed to meet VA's mission by providing a single integrated information system for Veterans health information in a single national information system.

Legacy VistA is reliant upon VistA logon capabilities to maintain system security. As VistA migrates to a Service Oriented Architecture (SOA), responsibility for Authentication and Authorization will move to the Enterprise Messaging Infrastructure (eMI). SSO capability will be provided by VA's IAM service, while authorizations will be maintained within the eMI. This same architecture will be implemented in Open Source VistA. While VA is using a proprietary product for the eMI, Open Source VistA will have the capability of using either proprietary or open source messaging infrastructures to provide the same capability. This refers to a desired end-state; the business rules for eMI to enforce authorization on requests are to be developed. Until these rules are developed, authorization, enforced by existing access logic, will reside within VistA.

The Privacy and Security Enterprise Design Pattern provides best practices for application architectures to use IAM services. The (Enterprise Architecture) Enterprise SOA Enterprise Design Pattern increment¹⁸ assisted migration of VistA to a SOA environment. The migration used ESS and the product planning roadmap, in accordance with the (Enterprise Architecture) SOA - VistA Evolution Enterprise Design Pattern increment.¹⁸

4.4 Transition Activities to Address Information Management Gap

An enterprise ADS does not exist. This results in the need for Veterans to provide VA the same information on multiple occasions. The duplicative data incurs extra costs to store, maintain, and backup. VA is undertaking several related initiatives to address gaps in information management.

4.4.1 Managing Data as an Asset

The collection, management, and distribution of information from source to audience, such as employees, clients, or partners, is essential to supporting and maintaining a customer-centric environment for government agencies. VA stores a vast amount of benefit, health, and memorial information; the proper management of this information is important to Veterans and employees.

Through robust Information Management, VA plans to support exponential growth in the volume and speed of data storage, retrieval, and analysis. This level of support will enable smooth navigation for Veterans across the VA network of services. Key transition activities related to information management are listed below.

- Ensure that VA systems use the Master Veteran Index (MVI) for basic Veteran data.

¹⁸ (Enterprise Architecture) Enterprise SOA Enterprise Design Pattern. Department of Veterans' Affairs. http://www.techstrategies.oit.va.gov/docs_design_patterns.asp

- Support information interoperability and semantic harmonization via a real-time mediation service.
- Implement robust information interoperability standards.
- Provide support to current and future clinical information exchanges with DoD for EHRs. The current system for EHR exchange is the Bidirectional Health Information Exchange (BHIE), which is being transitioned to the Defense Health Management System (DHMS) Modernization Health Information Exchange and will be completed by FY18.¹⁹
- Realize information transformation through institution of VA-wide policies and procedures, and through an operational environment that is Customer Data Integration driven.
- Establish the VA EA Enterprise Logical Data Model (ELDM) to share across VA a common vocabulary and understanding of data concepts. Integrate the ELDM with other VA EA Administration and solution artifacts as the foundation to managing enterprise data. Leverage ADS when migrating to an operational environment.
- Utilize Non-Structured Query Language (NoSQL) constructs, in addition to existing technologies, to support unstructured data within VA, while complying with VA security guidelines.

4.4.2 Electronic Claims Processing²⁰

In FY13, OI&T began a phased-in approach to implementation of the Veterans Benefits Management System (VBMS). The agile development and execution of VBMS has helped to process claims more efficiently and eliminate the benefits claims backlog.

As VBMS evolves, new functionalities will become available. The goal of VBMS is to provide the technology infrastructure needed to reduce the average disability claim processing time to 125 days. Currently, about 75% of the claims inventory at the Veterans Benefits Administration (VBA) is in digital form for electronic processing. The replacement of the paper-based claims processing system with the VBMS automated process has resulted in a 45% to 60% productivity and quality improvement. When VBMS is fully developed, it will enable end-to-end electronic claims processing across each stage of the claims lifecycle.

4.4.3 Enterprise Analytics

The VA regional analytics solutions no longer adequately support the data needs at VA. The Department requires enterprise analytics and big data capability that align with emerging business and technology environments. Enterprise-level governance and management groups for VA analytics lay the necessary groundwork for establishing this type of capability. VA's

¹⁹ Vista Evolution Program Plan. Department of Veteran's Affairs. March 2014.

https://www.osehra.org/sites/default/files/vista_evolution_program_plan_3-24-14.pdf

²⁰ CIO Annual Report. Department of Veterans Affairs. 2013 (Draft).

Business Intelligence Service Line (BISL) and the governance boards of BISL's Information and Analytics Ecosystem will be able to serve in this role with appropriate policy support.

The Analytics Ecosystem has developed effective approaches to sharing data, and for provisioning analytics tools and environments as enterprise services. BISL, which manages the Ecosystem, is able to connect existing warehouses and future advanced analytics capabilities to the Corporate Data Warehouse as loosely coupled "enclaves." Connecting current regional analytics capabilities to the Analytic Ecosystem provides VA with much-needed cross-cutting data collection and sharing capabilities for enterprise programs established under the MyVA strategic initiative.

4.4.4 Integrate Master Veteran Index for all VA Systems

MVI's data stewards, Healthcare Identity Management, are responsible for maintaining and operating the ADS that supports all of VA's IAM services. Unfortunately, they do not have the authority and staffing resources necessary to act as providers of an ESS. As a result, many VA applications and systems are either not integrated with MVI or do not use it correctly.

4.5 Transition Activities to Address Interoperability Gap

Currently, VA exchanges information with external partners using point-to-point interfaces, which creates duplicative instances of information sharing. For example, applications under development do not have shared services available, causing non-standard user interfaces, data exchanges, performance monitoring, and security implementations. VA is undertaking several related initiatives to address gaps in shared services.

4.5.1 Enterprise Shared Services

ESS is an enterprise direction for software services at VA, with the goal of advancing VA's organizational agility via the reuse, interoperability, and governance of IT services across internal and external organizational and program boundaries. This initiative also serves as a catalyst for applying a VA-wide IT services approach to move VA away from stove-piped, system-specific solutions toward enterprise IT solutions.

VA OI&T is leading an IT ESS Initiative that facilitates an effective and cohesive implementation of an enterprise service-oriented paradigm. This involves working with business leaders to identify business capabilities that include specific logic and business rules, as well as governance of those rules, in order to facilitate promotion of business capability-aligned software services into IT systems. Shared services will promote orchestration, authentication, and authorization attribute management, and data access IT services throughout the enterprise. New business capabilities will be created rapidly and economically with increased consistency and commonality across VA. Key transitional objectives related to ESS include:

- Cross-organizational information and functional capabilities available through IT shared services.
- Vertically integrated systems transitioned to reusable IT services and capabilities.
- Capabilities and services deployed consistently throughout the enterprise.
- Common services to facilitate rapid solution assembly.
- Enterprise approach for IT service governance.
- Enterprise policies, procedures and practices to govern IT services identification, usage and deployment.
- Environments for tools and techniques to support planning, development and operation of enterprise and business sector IT shared services.
- Implement the eCRUD service and operational data lake for the VA EA data layer.

VA established an ESS Center of Excellence (ESS-CoE) in support of the IT ESS initiative. The ESS-CoE provides a single focal point of SOA leadership across VA Enterprise for aligning and combining SOA resources and applying them to key areas. The ESS-CoE facilitates and accelerates the overall SOA adoption process and the creation/usage of ESS across VA, its partners, and customers. As a focal point, the ESS-CoE will assist in aligning business needs (defined by the business) with IT ESS's and VA OI&T's realization of a service-oriented solution strategy. This service strategy is intended to propagate SOA principles and best practices that apply to IT services, whether or not they are ESS candidates.

The benefits of applying an ESS-CoE are:

- Acceleration of SOA skills development and knowledge transfer allowing an organization to efficiently develop new services and enable those services to support new business capabilities.
- Common approach and techniques across OI&T teams promoting interoperability and consistency across disparate application platforms and technologies.
- Visibility and access to SOA resources across VA, other agencies, and external partners encouraging SOA adoption and socialization.
- Metrics to enable the measurement of VA ESS SOA adoption and common services deployment success.

4.5.2 Veterans Health Information Systems and Technology Architecture

MyVA's goal is to transform VA into an organization capable of providing Veterans with a single, comprehensive benefits delivery solution. Each Veteran will have a single, approved longitudinal health record to achieve interoperability with DoD and other healthcare partners.

For Veterans, the plan will begin with inception into service, and move with them through each stage of active duty, eventual separation or retirement from service, and Veteran status.

Interoperable EHR systems will improve the speed and accuracy of clinical decision making and ensure that authorized beneficiary and medical data are accessible, usable, shared, and secure. Patient safety will be improved as critical clinical findings will not go unresolved. Standardization of terminology across DoD/VA will promote accurate monitoring and management of an individual Veteran's care, and will enable cross-Agency data analysis and research to address service related diagnoses.

Achieving interoperability with other systems, such as the Social Security Administration, will enhance Veteran access to the full range of available benefits and services.

New VistA services will benefit from modern technologies and architecture to allow Veterans to access health information and benefits through a wide variety of devices (e.g., desktop browsers, smartphones). The VistA Evolution Program will oversee VistA's future adherence to SOA Enterprise design principles. This will result in a vendor-agnostic technology platform that is highly responsive to changing clinical needs. By modifying or replacing existing systems, new functionality can be added as new services, and old functionality can be updated. Other applications will connect through the middle-tier components, such as VistA Exchange, to reach patient-related information that is accessible through the Enterprise File Manager (FileMan), VA Exchange, and the outpatient-appointment scheduling system. These enhancements will allow Veterans to access health data quickly and easily from a wide variety of devices.

FileMan is the interface to provide structure for the data in VistA's database. Planned future enhancements to FileMan will enable querying and aggregation of structured data between VistA databases. Upgrades to FileMan will allow the federation of records from multiple systems to create a virtual database, with support for table-driven record movement and deletion.

VistA Exchange is a data management and messaging engine that will provide aggregated and normalized data, along with a data cache that will significantly enhance performance and reduce redundant network traffic. VistA Exchange will provide a longitudinal health record, also known as an enterprise Virtual Patient Record, which natively integrates data from VistA instances and from DoD and third party providers. VistA Exchange was part of the Enterprise Health Management Platform Release 1.0, which was delivered and deployed to the AITC EDE in September of 2014.

VA must ensure that its EHR systems are interoperable with DoD EHR systems, provide an integrated display of data, and comply with national standards and architectural requirements, as identified by the Interagency Program Office. VA must meet the following requirements by December 31, 2016:

- Deploy modernized EHR software that achieves Generation 3 level or better.

- Deploy modernized EHR systems capable of supporting clinicians of both Departments.

The VistA Evolution Program will deliver VistA 4's capabilities in four Feature Sets. The first Feature Set was successfully delivered at the close of FY14. The capabilities delivered in Feature Set 1 are listed below.

- Interoperability: Joint DoD/VA information sharing through the Joint Legacy Viewer.
- VistA Standardization, Phase 1: The two Feature Set 1 sites were standardized on the 74 VistA products of the Interagency Interoperability Core Product Set. Work on VistA Standardization consists of multiple phases, which span multiple FYs and Feature Sets, with work scheduled for completion by the end of FY15.
- VistA Immunization Enhancements, 1.0: Upgraded VistA files to allow use of standardized data and capabilities to read and write immunizations.
- Laboratory: The newly awarded System Engineering & Integration contract provides architecture, requirements design and Concept of Operations support for Laboratory. One or more Laboratory Enhancements project(s) will be initiated in Feature Set 2 to address priority funded enhancements to VistA Lab.
- Graphical User Interface (GUI) Tools: Added functionality will be added to the clinical GUI which includes: Google-like searches across an entire patient record, InfoButtons that provide context-specific knowledge resources for medications and patient education, improved medication reviews for enhanced safety, tasks for team-based coordination and follow-up, and a Newsfeed for rapid, chronological review of a patient's care and results.
- VistA 4 API, 1.0: This release identified an initial set of VistA APIs to expose as services via standard web services programming interfaces. Further work will take place in API Exposure, 2.0.
- Approximately 226 APIs were identified to be developed as services on the Enterprise Service Bus and Service Registry/Service Repository. Exposing an API as a service allows an application outside of the M-Code (Massachusetts General Hospital Utility Multi-Programming System Code) environment to use a Remote Procedure Call (RPC) to invoke a VistA API. APIs, exposed as a service, provide complete, secure, and unambiguous access to information in the selected VistA packages. Full exposure of these services will take place in API Exposure 2.0.
- Enterprise Messaging Infrastructure: eMI, the sustainment phase of the SOA suite project, will facilitate the delivery and use of reusable services in support of cross-Agency interoperability.

VistA will be a Generation 3 EHR enterprise-wide upon delivery of enterprise-wide capabilities in Feature Set 4. VistA 4 is being built upon SOA principles, design approaches, and the identification of common services. The inner workings of services are isolated (i.e., black box), and can potentially be changed with minimum impact to service consumers. This will increase

the flexibility for updates, enhancements and the expansion of individual system components, while minimizing the complexity of system-to-system communication. Overlaid with commons services, independent capability development teams can work autonomously to construct complex processes.

Exposing an API as a service allows an application outside of the M-Code environment to use a RPC to invoke a VistA API. APIs, exposed as a service, provide complete, secure, and unambiguous access to information in the selected VistA packages. External applications and systems can use VistA services in a 'plug and play' capacity – the more APIs that are published the more open the environment becomes.

4.5.3 Authoritative Data Sources

VA's Enterprise Information Management Policy states that OI&T will work with Administrations and lines of business to select and designate data stores as ADS. These ADS will be definitive "master records" for elements of commonly used Veteran data. VA only has one ADS (MVI, for identity traits). Designating additional ADS and integrating VA data stores will facilitate data interoperability by providing shared points of reference for the entire VA enterprise.

4.5.4 Enterprise Logical Data Model

The goal of ELDM is to establish shared conceptual, logical and physical data models for common Veteran data within VA. The ELDM will serve as the canonical data model for the proposed VA EA data layer (described in the (Interoperability and Data Sharing) Hybrid Data Access (HDA) Enterprise Design Pattern) and will enable communication and interoperability between VA's data sources in combination with designated ADS.

4.5.5 Implement the Enterprise Create, Read, Update, Delete Service and Operational Data Lake for the VA Enterprise Architecture Data Layer

The (Interoperability and Data Sharing) HDA Enterprise Design Pattern describes a VA EA Data Layer that facilitates interoperability and centrally manages VA data assets. The eCRUD service and Data Lake are two critical components of the proposed data layer. eCRUD supports encapsulation and consistent management of assets within the data layer, while the Data Lake serves as a hub for data transformation, cleansing, normalization, and other operations that are necessary for data aggregation and interoperability.

4.6 Transition Activities to Address Mobile Gaps

VA's current Domain specific infrastructures, standards, data and application interfaces limit a mobile enterprise environment. VA is undertaking several related initiatives to address gaps in the mobile environment.

4.6.1 Mobile Architecture

Mobile technology continues to advance at a rapid pace causing a greater emphasis on enabling an increasingly mobile workforce to access high-quality digital government information and services anywhere, anytime, and on any device. Mobile broadband subscriptions are expected to grow from nearly 1 billion in 2011 to over 5 billion globally in 2016. By 2015, more Americans will access the Internet via mobile devices than desktop personal computers.²¹ As new technologies are introduced, policies governing identity and credential management need to evolve to allow new solutions that address the dynamic mobile world.

VA is establishing a long term strategy to provide guidance toward a common end vision; shifting from the traditional desktop to mobile devices to support the staffs' everyday needs by providing an adaptable environment to support the enterprise. VA is piloting new mobile products, TRM's automatic application review, network access controls integrated with a mobile device manager, and Geo-location proximity-sensing capabilities for mobile devices. Key transition activities related to Mobility encompass integration of the mobile strategy into IT initiatives.

4.6.2 Enterprise Mobility Management²²

Enterprise Mobility Manager (EMM) aims to establish a minimum baseline on devices that need to access enterprise information across VA. VA EMM has general capabilities to manage devices and applications, both VA and non-VA owned. Some VA EMM capabilities include:

- Setting complex passwords.
- Delivering and removing applications.
- Reviewing all applications on the devices (not data within the application, but the application list itself).
- Delivering and removing VPN Profiles, VA Intranet, Wi-Fi Access, etc.

4.6.3 Mobile Device Management

In FY14, VA OI&T leveraged the Mobile Device Management (MDM) tool for advancement of VA's mobile capabilities by deploying close to 10,000 new Government Furnished Equipment (GFE) mobile devices to VA staff. Staff were enabled management, configuration, and security for iOS and Android mobile devices. Mobile devices are the foundation for numerous applications being developed to provide secure access to VA's core business lines. The MDM provides a secure baseline through the visibility and management of the devices, to holistically secure and control the device, to manage passwords and encryption, to create different accounts, and to remotely wipe data if a device is lost. The MDM is being integrated into other tools to provide additional enhancements around security visibility with the addition of an

²¹ Digital Government Strategy. The White House. May 23, 2012. <https://eapad.dk/gov/us/digital-government-strategy/>

²² Information Security Webinar Series: Mobile Device Security. The Department of Veterans Affairs. December 14, 2015.

endpoint status of a visibility dashboard. The MDM delivers certificates to the device providing staff access to VA's secure wireless network and secure remote access. Finally, a new pilot is being employed to test the traditional endpoint model with mobile tablets, to reduce the device footprint and provide secure access to staff regardless of location. MDM can provide increased functionality to:

- Advance VA health care by developing solutions leveraging mobile devices.
- Provision a mobile version of VistA with encryption, enabling the secure uploads of medical records from tablets or other mobile platforms.
- Consolidate mobile email using secure routing to VA's Mobile Framework.
- Develop collaboration tools to leverage mobile devices, and integrate with VA's traditional endpoints.

4.6.4 Mobile Application Management

Mobile Application Management (MAM) aims to manage mobile applications (not the full device) for controlling and securing access to VA information and resources. MAM is the solution to Veteran Facing Applications and the potential deployment of a Bring Your Own Device (BYOD) program for VA.

MAM creates a container on the device where all enterprise applications tied to the EMM reside. Applications can be removed if the user ends their service at VA, if the device falls out of compliance, or is lost. In the future, VA will be able to use container technology to automatically push work applications into a protected environment on the device.

Long-term goals of VA MAM include:

- Progress device agnostic.
- Develop best practices for Mobile Enterprise Applications.
- Support VA BYOD Program.
- Leverage VA's VPN security practices.
- Acquire automated application risk analysis tools.

4.7 Transition Activities to Address Application Modernization Gap

The current IT environment consists of a diverse infrastructure with modern and legacy technologies. VA's distributed computing environments are characterized as tightly coupled systems which would benefit from integrated design, ability to reuse existing IT investments, and industry standards. VA is undertaking several related initiatives to address application modernization gaps.

4.7.1 Open Source

Open source refers to software in which source codes are publically available for use and modification from the original design. The controlled source codes are available by the provider for users to modify and redistribute to develop additional software capability.

VA has and will continue to embrace applications and programs that take advantage of an open source model, which invites innovation from the public and private sectors.²³ The Federal government is fully committed to building a 21st-Century Open Government, continuing to work with various public and private partners to effectively harness the expertise, ingenuity, and creativity of the American Public by enabling, accelerating, and scaling the use of open innovation methods across the government.²⁴

VA is establishing requirements to thoroughly evaluate Open Source Software (OSS) solutions when VA acquires software, and to consider the use of OSS development practices when VA develops software.²⁵ VA recognizes numerous potential advantages to utilizing and relying upon OSS solutions in support of VA's mission. Potential advantages of OSS solutions include lower development costs, lower licensing costs, lower maintenance costs, faster introduction of community developed innovations, higher software quality, and increased openness and transparency.

Effective January 1, 2015, planning and execution of VA software projects will consider OSS solutions, in addition to proprietary software solutions, when acquiring software systems. The considerations outlined above will be evaluated and documented in addition to current software evaluation metrics, resulting in a comprehensive analysis of advantages and disadvantages when conducting software acquisitions. VA software development projects, whether performed by VA or with the support of contractors, will consider the use of OSS development practices.²⁵

4.7.2 Veterans Health Information Systems and Technology Architecture

The VistA team is collaborating with innovators through multiple outreach efforts with the open source community. For example, the VistA Intake Program assists members of the global VistA community to work with VA to rapidly bring field-developed code to Class 1 code, that is suitable for use in the VA environment.

²³ VA Launches Open Source Custodian. Veterans Today. August 30, 2011.

<http://www.veteranstoday.com/2011/08/30/va-launches-open-source-custodian/>

²⁴ The Open Government Partnership, National Action Plan for the United States. The White House. September 20, 2011. http://www.whitehouse.gov/sites/default/files/us_national_action_plan_final_2.pdf

²⁵ Memorandum: Consideration of Open Source Software. Department of Veterans Affairs CIO. Nov 4, 2014.

http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=804&FType=2

VA has relationships with World VistA and Hardhats. WorldVista is a non-profit organization designed to assist healthcare entities who wish to use VistA outside of VA. Hardhats is a collaborative group focused on VistA development and documentation.

VistA is bound by the Open Source EHR Alliance (OSEHRA), the central governing body that oversees the community of EHR users, developers, and service providers that will deploy, use, and enhance the EHR software. OSEHRA created a centralized, robust, and completely open source framework, promoting the stabilization, refactoring, and modernization of VistA. In addition, a Code Repository and Software Quality Certification Process has allowed OSEHRA to provide the community with robust tools enabling users, developers, and researchers to engage with and advance EHR technology.

Another example of VA's commitment to open source is the new PD program called Code in Flight, which was created to share VA project artifacts with the open source community during enhancement of health products. This marked a change from the previous VA policy on the Freedom of Information Act (FOIA) releases, to share only nationally deployed products. It created project management procedures that were placed in the OI&T process management tool. It developed five process phases as project collection points and targeted artifacts in Project Planning, Product Design, Product Build, Test, and Independent Test and Evaluation. In FY13, 41 PD projects were identified as enhancing or extending VistA Health products and were targeted for Code in Flight releases during the development period. By the end of FY13, 21 development projects were successfully shared as Code in Flight.

In FY14, OI&T increased the number of health products shared with the community during development phase, and addressed additional necessary changes to design standards, documentation standards, and FOIA procedures. These initiatives allowed OI&T to increase the throughput of releasing to the open source community. They widened the channel and increased the number of pilot projects to intake open source developed, or modified health products, into the VA environment.

4.8 Transition Activities to Address Collaboration Gap

VA has a need to provide centralized, enterprise-grade collaboration services for IT governance, content and records management, and enterprise portals. VA is undertaking several related initiatives to address gaps in collaboration.

4.8.1 National Service Desk

Since the inception of the NSD, the field service desks that were identified as requiring transition have been realigned to the NSD. Rollout of the Single Service Desk Phone System has been completed on time. A single point of contact has been established to serve OI&T users, providing one of the first enterprise level IT services in OI&T.

For example, the rollout established a single ticketing system for tier 1 Service Desks and business partners. This system provides a single repository to manage and monitor trends in the OI&T enterprise (i.e., Requests for GFE or teleworking). This will allow the Service Desk to be proactive. In addition, NSD has established a swift action and triage process to remediate critical incidents within OI&T. The NSD project is in sustainment; it has identified a process improvement plan that includes reviewing the vision and plans on an annual basis.

4.8.2 Next Generation Satellite Communications

The Next Generation Satellite Communications program provides contingent voice, video, and data communications services via IP for desktop and mobile applications that provide satellite-based voice, video, and data communications services. Many VA program offices will use this satellite delivery system, including three OI&T groups: OI&T Leadership, OI&T Emergency Preparedness (Support Service Line Managers), and data centers.

4.8.3 IP Video to Home National Expansion

OI&T, in conjunction with VHA's Office of Telehealth Services, provided virtual care to 15,000 Veterans in FY13, enabling Veterans who have difficulty traveling to obtain care. The program has a target to provide virtual care services to all Veterans by the end of FY15. Virtual healthcare services provide clinical consultations, including video sessions. The virtual services transfer patient vital signs data and electronic medical records to clinicians.²⁶

4.8.4 Voice as a Service

Voice-as-a-Service (VaaS), commonly referred to as 'internet phone', is the use of IP-based networks to route voice communication over the internet. VaaS digitizes voice information and live conversations for rapid transmission over the internet, rather than phone lines. VaaS provides better quality of service and reduces costs.

Voice service is a foundational component in business communications. Like many organizations, maintenance of the VA infrastructure has become an ever growing and unsustainable portion of the budget. The traditional Private Branch Exchange (PBX) voice systems contribute to the rising infrastructure costs, as many of the systems are more than 15 years old and cannot be adequately maintained.

Over the last several years, OI&T has developed the Enterprise Voice System, also known as the VaaS project. The intent of VaaS is to modernize the voice infrastructure within VA, while providing cost savings, using a hybrid of Government Owned and Contractor Operated (GO/CO) systems.

Part of the GO/CO strategy is to centralize the control of voice systems under a centralized management tier, providing unified communications features to end users, without a costly

²⁶ CIO Annual Report. Department of Veterans Affairs. 2013 (Draft).

upgrade to current PBX systems. There is currently a GO/CO proof of concept effort underway at three locations within VA (Fort Harrison, Montana; Tennessee Valley Health Care System, Tennessee; and Charleston, South Carolina). The intent of the proof of concept is to demonstrate that the GO/CO strategy is productive and provides cost savings to VA, enabling the Department to implement the system across a broad spectrum over the next several years, and eventually, encompass the entire VA voice system.

4.9 IT Consolidation Efforts

4.9.1 Data Center Consolidation

In response to the OMB FDCCI²⁷, VA has developed a data center consolidation approach to optimize and consolidate decentralized health record systems across VA Regions 2 and 3, into two enterprise level data centers. As part of that approach, VA has migrated 12 production health record systems to Defense Information Systems Agency Defense Enterprise Computing Centers. Additionally, VA is in the planning stage for virtualizing and optimizing the infrastructure and architecture for VA Region 1 and 4 health record systems, that were consolidated prior to 2009.

4.9.2 Ruthless Reduction Task Force

In response to the 2011 Promoting Efficient Spending Executive Order, OI&T established the Ruthless Reduction Task Force (RRTF) to explore ways to reduce costs and increase the rate of return on every tax dollar invested in IT.

RRTF promotes, identifies, analyzes, designs, and recommends IT cost containment opportunities. RRTF focuses on the interactions and interdependencies of people, process, technology, policy, solutions, and user experiences to improve synergy, the combined efforts to reduce or eliminate expenses, and avoid duplication. The task force aims to improve operational efficiencies and contain costs, by analyzing day-to-day processes and procedures, policies, best practices, and standards for running an enterprise.

Through the development of training and communication, RRTF promotes stewardship among VA stakeholders, the responsible planning and management of resources. The task force promotes an ethical responsibility to look aggressively for IT optimization and cost containment opportunities.

²⁷ Federal Data Center Consolidation Initiative. Office of Management and Budget. February 26, 2010. https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal_data_center_consolidation_initiative_02-26-2010.pdf

RRTF has executed cost containment opportunities by (1) decommissioning redundant systems; (2) consolidating development and test environments; (3) implementing SOA, data center consolidation and cloud computing; and (4) creating efficiencies in obtaining security approvals for onboarding employees and contractors.

As a result, the task force aims to identify efficiencies for re-purposing greater amounts of appropriated funds to development, modernization, and enhancement to meet emerging VA priorities. To do so, RRTF closely analyzes industry best practices and modernized IT systems and technologies. These efforts allow for better resource allocation without impacting safe, reliable, service delivery to Veterans and support for internal VA management processes. Between 2012 and 2014, RRTF tracked approximately \$87 million in cost savings from the renegotiation of VA's enterprise-level agreement (ELA) with Microsoft. Since the Microsoft ELA contract extends to 2017, VA will still realize an additional cost savings of \$37 million in 2015 and \$37 million in 2016, for a total of \$161 million in cost savings.²⁸

In 2015, RRTF was engaged with multiple workstreams, including Modeling and Analysis, Performance Measurement, Systems Divestiture, Operational Capabilities Assessments (OCA), Communications, Process Improvement, and Training. These workstreams include analysis of VA OI&T systems such as BHIE, Desktop Database Management Systems, VA System Inventory, Configuration Management Database (CMDB), and TRM.

RRTF reviews multiple distinct systems within VA OI&T as potential cost containment candidates. These tasks will eventually develop into full scale projects to align with and be implemented in support of VA's goals. The performance measurement framework analyzes RRTF initiatives to identify potential cost saving opportunities and to assess how appropriately the budget is being disbursed. The OCA methodology is used to identify gaps in processes, technology, strategy, and architecture within the organization. An Analysis of Alternatives (AoAs) helps justify the need for starting, stopping, or continuing an acquisition program. AoAs identifies potentially viable solutions and provides comparative cost, effectiveness, and risk assessments of each solution to a baseline; this baseline is typically the current operating system. AoAs also provides a foundation for developing operational requirements, concepts of operational employment, a test and evaluation strategy for the preferred alternative(s), and additional information for the program office when one is formed. RRTF strives to make recommendations that will include activities that contribute to the improvement of information resource management in a repeatable and sustainable manner.

OI&T has already implemented some of the RRTF recommendations, such as renegotiating major enterprise licenses, and eliminating dedicated servers through virtualization. OI&T has

²⁸ RRTF Common News Newsletter. Department of Veterans Affairs. May 2015. http://vaww.blog.va.gov/rrtf/wp-admin/post-new.php#_ftn1

also initiated RRTF recommendations, such as establishing a mobile device policy to reduce the number of devices being issued, and eliminating desktop printers.

- **Server Virtualization Initiative**²⁹ – VACO IT Support Service has continued to expand on server virtualization, directed by OI&T’s SDE office, by replacing old systems and consolidating servers in a centralized location. The Server Virtualization Project reduces hardware support costs, minimizes the carbon footprint, and improves data access times. Reducing physical servers wherever possible and virtualizing them is estimated to save VA more than \$9.2 million over FYs 2014 and 2015. Replacing physical servers with virtualized servers is estimated to yield a cost benefit of approximately \$13,000 per server, based on new physical server cost. By the end of FY13, server virtualization increased 60%-70%.

5 VA PROCESSES SUPPORTING TRANSITION

VA developed processes to help guide OI&T from the current to the future state of IT. The technical layer of the VA EA, known as the ETA, defines the IT infrastructure environment required to support the VA business application environment and achieve VA mission requirements. The ETA is a set of architecture products detailing reusable standards, rules, guidelines, and configurations for the enterprise IT layer of the VA EA. The ETA will inform and govern the development, deployment, and maintenance of IT hardware, software applications, systems, and networks by:

- Integrating technical guidelines from across OI&T and making them available to stakeholders via the VA EA.
- Defining systems, services, infrastructure, and security compliance requirements using standardized methods and formats.
- Enabling IT compliance, governance, and enhanced decision support capabilities.
- Applying enterprise goals and strategies during the Solution Design processes.

VA published policies and architecture products to document rules and standards for the ETA, as illustrated by Figure 5. These documents include the Enterprise Application Architecture, Infrastructure Architecture, Conceptual Data Model, SOA Technical Framework, and VA 6500 Information Security Handbook. Collectively, the rules and standards in these documents ensure interoperability of VA’s IT environment and integrate new applications to provide seamless service to Veterans.

²⁹ CIO Annual Report. Department of Veterans Affairs. 2013 (Draft).

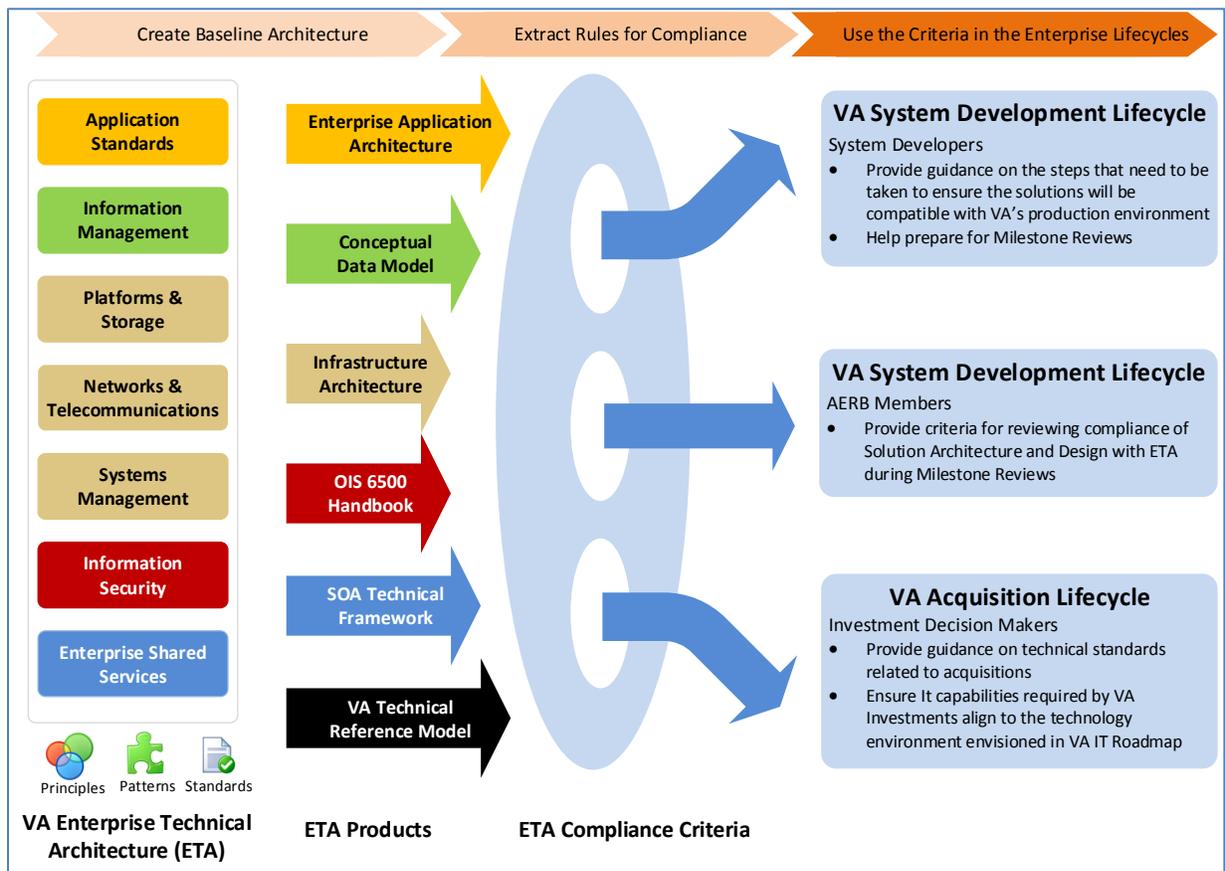


Figure 5: VA Enterprise Technical Architecture (ETA) Compliance

5.1 Enterprise Technical Architecture Compliance Criteria

To ensure interoperability of solutions and transition IT capabilities to the technology environment envisioned in the ETSP, the ETA Compliance Criteria contains architecture rules that describe how VA's IT environment must be designed and configured. The purpose of ETA Compliance Criteria is to ensure alignment of VA programs, projects, initiatives, and investments with the VA ETA. It details rules and standards for use and configuration of VA networks, as well as standards for information security and application design.

5.2 Technical Reference Model

The VA EA TRM is one component within the overall VA EA that establishes a common vocabulary and structure for describing the IT that is used to develop, operate, and maintain enterprise applications.

TRM provides a meaningful framework to identify and analyze emerging technologies, identify how these technologies can impact VA operations, and determine what is needed to achieve

successful implementation within the VA IT environment. TRM includes the Standards Profile and Product List, and serves as a technology roadmap and tool for supporting OI&T.

VA employees and contractors are required to use the VA EA TRM site at <http://va.gov/TRM> to determine technical alignment and the decision status of technologies. The TRM also contains standards directed by the Principal Deputy Assistant Secretary for Information and Technology and is part of the project management process. The TRM site provides instructions for submitting new technologies to be evaluated and included in future releases of the TRM. Users can search for technologies, generate reports, review forecasts, and access the release history of technologies. TRM also provides training to users at all levels through its training course on the VA Talent Management System (TMS).

5.3 Enterprise Design Patterns

Enterprise Design Patterns are capability guidance documents that identify repeatable, best practice approaches to address recurring technical problems. Employing Enterprise Design Patterns helps VA to improve and evolve information security, advance interoperability and information sharing, and reduce IT lifecycle costs. They help project-level PD activities by enabling enterprise capability reuse provided by a shared, enterprise-wide IT infrastructure. Enterprise Design Patterns provide architectural context and constraints to inform VA system design, referring to standards, guidance, and policies. Projects will refer to Enterprise Design Patterns to identify design constraints in accordance with the VA ETA, and use approved tools and technologies specified in the TRM.

Approved Enterprise Design Patterns were developed in an open, collaborative environment that includes internal and external stakeholders and subject matter experts, in order to achieve enterprise-level consensus. These documents are developed iteratively, culminating with a final version that is agreed upon in a Public Forum meeting; and the documents are subsequently approved by ASD leadership.

Enterprise Design Patterns will simplify developing applications, allowing projects to concentrate on front-end development using responsive design techniques and PaaS models. Enterprise Design Patterns relieve project teams of the burden of developing application-specific back-end resources. Projects subject to the project management process are required to assert adherence to Enterprise Design Patterns prior to lifecycle initialization, and to evaluate published Enterprise Design Patterns as they progress through the project management process lifecycle.

Enterprise Design Patterns align to infrastructure gaps delineated in the ETSP (represented in Table 5). Table 7 provides a description of the Enterprise Design Patterns. Approved Enterprise

Design Patterns are published on the following TS website:
http://www.techstrategies.oit.va.gov/docs_design_patterns.asp.

Table 7: Enterprise Design Pattern

Design Pattern	Description
Privacy and Security	Provides capability guidance that identifies best-practices to solving reoccurring enterprise level security and privacy problems within the VA
Enterprise Architecture	Provides the overarching construct to guide VA toward a common set of cross-platform SOA capabilities, leveraging ESS and enterprise-grade computing platforms
Interoperability and Data Sharing	Provides strategic guidance for VA to develop and implement the governance, processes, and technical capabilities necessary to support enterprise-wide data interoperability, visibility, and accessibility
IT Service Management	Provides strategic guidance on the processes established by VA to implement enterprise-wide IT asset management capabilities including configuration management of services in the IT infrastructure, in accordance with approved tools and technologies located in the TRM
Mobility	Provides guidance to projects developing mobile applications aligned to enterprise mobile capabilities and infrastructure to access VA IT resources and external systems relevant to the VA through mobile devices for internal and external users
Cloud Computing	Provides guidance to projects on leveraging cloud capabilities aligned to VA’s Cloud Strategy

5.4 Enterprise Management Framework

VA’s EMF is a system designed to collect data from across VA and provide for the management and reporting of VA IT data from a single federated repository. This system consists of numerous servers and COTS products. The servers and COTs products are integrated together in a customized fashion in order to provide a view of federated assets and IT information across VA.

VA constructed the EMF system to provide centralized management of the complex enterprise infrastructure. The EMF includes a Federated Data Repository (FDR) as the centralized reference location for VA Managed Data Repositories (MDRs). With an Open Database Connectivity and a Java Database Connectivity connection with MDRs, VA can map and extract information from various distributed data sources.

The FDR includes capabilities to create management reports, provide intelligent analysis and trending, and enhance the ability to "view" IT data from a single data source. The FDR

incorporates a CMDB and system, in support of the IT Infrastructure Library. Through a customized software connection, over 80 data sources (MDRs) are connected to the EMF FDR. The EMF FDR leverages data from MDRs throughout the enterprise to present a national view of data and critical service management; and to provide enhanced release, configuration, change, and incident management.

5.5 IT Governance

The EA Council (EAC) oversees the development and implementation of the VA EA and provides the means to monitor, control, and report on technical changes impacting architecture and VA business customers. At the tactical level, the EAC has three sub-working groups, the AERB, the EA Working Group (EAWG), and the ETA Working Group (ETAWG). All three report to the EAC. The ETSP, including the IT Vision, was created with support from the working group members of the EAC, EAWG, AERB and ETAWG.

The AERB serves as the governing body between functional planning and IT Strategy. It provides oversight, governance, coordination, and a comprehensive control process that minimizes conflicts and duplication of efforts among IT initiatives.

As part of the VA project management process, the AERB is responsible for reviewing and approving Milestone documentation. The project management process requires IT investments to develop and provide documentation in three major areas: alignment with the VA EA and business, technical plans, and project management plans.

ASD is in the process of developing a plan to insert the VA EA and VA IT strategy earlier, within the AERB and project management processes. Earlier project management process engagement drives the IT Vision forward and ensures compliance with the rules, standards, and policies of the VA EA. To ensure that IT deployments are aligned with enterprise level guidance for established solutions, Enterprise Design Patterns should also be introduced at this point. The result will be a well-defined project plan, ensuring that planned technologies are approved in the TRM and reducing potential waiver requests to the AERB. ASD is developing a strategy to resource this effort with subject matter experts across the organization.

6 IMPACTS ON IT TRANSITION EFFORTS

Multiple internal and external factors influence how VA develops, deploys, and prioritizes the transformation of infrastructure. These factors include changes in business goals, healthcare, or IT related legislation; federal or agency level guidance; and emerging technologies. These factors lead to changes in priorities, schedule, and budget. Below are some of the influences OI&T will consider as it plans an appropriate response to an ever changing environment.

6.1 Technology Trends

VA's IT infrastructure environment may be increasingly influenced by technological advancement. VA should evaluate alternatives, based on risk and economic justifications. VA has the potential to stay abreast of emerging technologies to produce timely and improved products and services, by seizing the opportunity to incorporate emerging technology trends³⁰ into future strategic plans. Leveraging these trends has the potential to assist the VA in developing a flexible and efficient IT infrastructure environment for the enterprise. VA needs to determine how it can take advantage of these trends and emerging technologies, in order to create innovative products and services that extend the reach and relationship to Veterans, service members, and internal customers.

6.1.1 Cloud/Client Computing

Cloud computing is becoming more mature and prevalent. Cloud services leverage outsourced, external computing resources that provide the ability to synchronize content, make applications portable, and ease the convergence of traditional and mobile computing.

Benefits: VA has the opportunity to utilize the benefits of cloud computing by moving towards a dynamic IT infrastructure that optimizes efficiency and flexibility. The adoption and implementation of a cloud computing model delivers benefits that address scalable infrastructures, cost savings from a pay-for-use model, and self-servicing capabilities. Cloud computing is a compelling technology for VA because it provides ubiquitous, elastic, and on-demand access to a shared pool of configurable resources, without investing in new infrastructure.

Cloud computing can help reduce operational cost by enabling the switch from a depreciative CapEx cost model to Pay-for-Use model, in order to drive cost savings and cost smoothing for certain functions. To meet rapidly changing demands, VA can transition from an extensive manual process for delivering IT capabilities, to elastically provisioned IT capabilities. This will help address the increasing demand for computer resources, ultimately leading to a quicker response to meeting the needs of Veterans.

Recommendations: Here are some steps OI&T can take to move forward with existing Cloud/Client Computing efforts:

- Continue to investigate transition of services to the cloud platform.
- Define VA's Enterprise cloud computing strategy.
- Track cloud technologies deployed and tested in the private and public sectors.

³⁰ Gartner Identifies the Top 10 Strategic Technology Trends for 2015. Gartner. October 8, 2014.
<http://www.gartner.com/newsroom/id/2867917>

6.1.2 The Internet of Things

“Simply put [the Internet of Things] (IoT) is the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other).”³¹ With a connectedness that was unimaginable only a few years ago, the IoT is rapidly being adopted, and the number of connected devices outnumber the world’s population by 1.5 to 1.³² The IoT is able to connect both inanimate and living things, use sensors for data collection, and change what types of items communicate over an IP network.³³

Benefits: IoT, as a rapidly emerging ecosystem of IP-connected devices³⁴, can deliver benefits through communication, control and automation, and cost savings. Since communication and connectedness exist among the devices within the IoT, and an automated process captures and stores vast amounts of meaningful data, information is provided that has never before been obtainable. In addition, due to the connectedness of the devices, IoT provides the ability for remote control and automation of devices.

Meaningful data, combined with advanced data analytic systems, has the potential to provide cost savings opportunities for VA by driving efficiency and automating processes that were previously labor intensive. It provides better products and services to Veterans by collecting and analyzing information, and putting knowledge at the fingertips of the right people at the right time.

Recommendations: The following steps can move OI&T forward with existing IoT efforts:

- Examine and track the implementation of a ubiquitous secure infrastructure (i.e., wired/wireless) that allows communication between disparate sensors and systems.
- To ensure that the environment can support a network of devices, continue to implement an IT infrastructure that supports mobility.
- Examine and establish policies and processes for data and security protection by implementing best practices and a risk based approach.

6.1.3 Computing Everywhere

‘Computing Everywhere’ refers to the use of interconnected devices to enable users to manage and access content across a variety of devices, from mobile, wearable, and kiosks, to traditional

³¹ A Simple Explanation of 'The Internet of Things'. Forbes. May 13, 2014.

<http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/>

³² The Internet of Things (IoT). Cisco. <http://www.cisco.com/web/solutions/trends/iot/overview.html>

³³ An Introduction to the Internet of Things (IoT). Cisco. November 2013.

http://www.cisco.com/web/solutions/trends/iot/introduction_to_IoT_november.pdf

³⁴ Cognizant: Reaping the Benefits of the Internet of Things. Cognizant. May 2014.

<http://www.cognizant.com/InsightsWhitepapers/Reaping-the-Benefits-of-the-Internet-of-Things.pdf>

computers, regardless of the type of operating system used. The VA vision seeks ubiquitous access to computing capabilities, in order to dramatically increase the availability of VA services to Veterans.

Benefits: The need for VA staff and Veterans to universally access information anytime, anywhere, and on any device, is fundamental to quality of life and optimum productivity in today’s hyper-connected world. Within VA, this access would shift support from a traditional desktop or laptop computing model, to a mobility model. It would redefine the workplace by streamlining business activities and optimizing device usage (i.e., BYOD policy), thereby improving employee productivity and the Veteran customer-service experience. By developing mobility-based electronic services that provide seamless access to the VA network from a multitude of devices, ‘Computing Everywhere’ can vastly improve the self-service experience for Veterans.

Recommendations: Here are some steps OI&T can take to move forward with existing Computing Everywhere efforts:

- Identify, document, and incorporate the workflow and device support requirements for VA staff, Veteran Service Organizations, and Veterans.
- Continue to investigate MDM tools that enforce security and compliance policies.
- Continue to investigate and develop cloud technologies and mobility strategies.

6.1.4 Software-Defined Applications

Software-Defined Applications represent a computing infrastructure that is entirely under the control of software, with no operator or human intervention, and with no hardware-specific dependencies. Rather than a single, self-contained unit architecture, software-defined applications are made of a number of independent components known as microservices, that communicate with each other via Application Programming Interfaces (APIs).

Software-Defined Applications utilize an architecture that introduces a level of virtualization between software producers and consumers. The virtualized boundary, also known as the Software-Defined Architecture Gateway, makes it possible to replace implementation, without directly affecting the consumer of the application. The gateway has an Inner API on one side, for the producer’s use, and an Outer API for the consumer. Services are used with Software-Defined Applications, but they are not consumed directly by Software-Defined Applications. Instead, the Gateway serves as the virtualized boundary and controller between the Inner and Outer API’s, separating a direct consumer-to-service connection.³⁵

³⁵ A New Style Is Emerging in the Enterprise: Software-Defined Architecture. InfoQ. May 24, 2014. http://www.infoq.com/news/2014/05/sda?utm_reader=feedly

Benefits: As Software-Defined Applications are the next logical evolution of the applications already developed by VA, using SOA, VA will be able to take advantage of security simplification, horizontal scaling, and automation. By creating a small number of services that interact directly with raw data, VA can reduce both the footprint, for possible security breaches, and the need for complex security mechanisms among services. Software-Defined Applications supported by Software-Defined Architecture are able to take advantage of horizontal scaling (ability to increase the capacity of existing hardware or software by adding resources), due to the flexibility introduced by gateway and inner and outer APIs. Finally, the API's within Software-Defined Applications, open a vast potential for automation within the application; and the Agile methodology in development of the application is strongly supported.

Recommendations: OI&T can take the following steps to move forward with existing Software-Defined Applications efforts:

- Build in-house expertise and culture around Software-Defined Architecture and Software-Defined Applications.
- Establish objectives for developing and deploying Software-Defined Applications.
- Clearly define and plan the architecture, with specific emphasis on the gateway, APIs, and services to support Software-Defined Applications.
- Properly plan and budget to avoid stovepipes.

6.1.5 Machine-Generated Data

Machine-Generated Data (MGD) is information that is automatically created from computer processes, applications, and other machines, without human intervention (i.e., computer or network logs, location data, sensor reading, and call detail records).

Benefits: MGD is a fast emerging and complex component of “Big Data,” with the potential to deliver valuable benefits to VA. These benefits include improved operational intelligence, historical data integrity, and a 360° perspective of consumers.

Through analyzing real-time dynamic business analytics, operational intelligence allows for real-time discovery that can help prevent cybersecurity attacks, reduce fraud, and improve Veteran experiences at VA. Analysis of VA's MGD showed a 360° view, with the unified view of Veterans' digital interaction with the Department, and the Department's digital interaction with Veterans. With this view, VA has the potential to monitor, respond to events, and improve the Veteran experience.

Recommendations: Here are some steps that OI&T can take to move forward with existing MGD efforts:

- Develop an analytic strategy for MGD to ensure VA is driving towards efforts focused around Veteran centric-outcomes that provide the most business value.

- Determine an enterprise-wide MGD strategy for how enterprise awareness of how data is intended to be used to improve business objectives.
- Examine data mining technologies.
- Examine the amount and effect of storage needs for the VA’s MGD.

6.1.6 Smart Devices

Devices such as activity monitors, sleep sensors, smart glasses, fitness monitors, smart clothing, pedometers, and smart watches are examples of smart devices. Smart devices generally connect to and interact with other devices, and have internet capabilities for enhanced functionality. Many of these devices enable patients to generate, monitor, and record their health data rapidly and routinely, and can assist healthcare officials in identifying serious health issues during patient care.

Benefits: Smart devices can significantly improve workflow by reducing task time, reducing the level of effort, or eliminating certain tasks altogether. Smart devices can connect patients to providers, enabling providers with immediate access to required information, and aiding in facilitating remote care.

Smart devices will allow physicians and clinicians to readily access diagnosis and procedure codes at the moment they are needed, and can insert them into the patient’s chart or bill. This eliminates common errors from a paper based process. Smart devices, such as wearable sensors, can monitor, track, and store a patient’s vital signs on a continual basis. The care giver will gain an accurate picture of the patient over time, which can lead to better diagnosis and treatment.

Recommendations: Here are some steps that OI&T can take to move forward with existing Smart Device efforts:

- Secure mobile healthcare devices and implement best practices.³⁶
- Understand and manage mobile smart devices used by health care providers.³⁷
- Implement technologies in the VA that can take advantage of the benefits from smart devices.³⁸

³⁶ Securing Mobile Healthcare Devices: Best Practices. InformationWeek. June 3, 2014.

<http://www.informationweek.com/healthcare/security-and-privacy/securing-mobile-healthcare-devices-best-practices/d/d-id/1269357>

³⁷ Five steps organizations can take to manage mobile devices used by health care providers and professionals. HealthIT.gov. January 15, 2013. <http://www.healthit.gov/providers-professionals/five-steps-organizations-can-take-manage-mobile-devices-used-health-care-pro>

³⁸ Mobile Devices and Apps for Health Care Professionals: Uses and Benefits. National Institutes of Health. May 2014. <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4029126/>

6.1.7 Context-Rich Systems

Context-rich systems leverage embedded intelligence and pervasive analytics. Context-rich systems are alert to their surroundings, enabling the system to respond with information that is valuable to the user, while eliminating irrelevant information and complexity. The information presented to the user is based on the context in which the user is interacting with that information.

Benefits: Developing and implementing context-rich systems has the potential to reshape how VA completes tasks and interacts digitally with the Veteran, their dependents, and Veterans Service Organizations. The benefits from a context-rich system can translate into easier system development, improved workflow, enhanced security, and enriched user experience. A context-rich system can understand and be responsive to different workflows, based on context. By understanding the context of a user request, a context-rich system can alter the security response and adjust how and what information is delivered to the user. By eliminating irrelevant information and complexity, the system greatly enhances the Veteran user experience.

Recommendations: Here are some steps that OI&T can take to move forward with existing Context-Rich Systems efforts:

- Develop expertise in the area of context aware systems.
- Attempt a small project that incorporates and exploits a context-rich system.
- Engage market leaders in the technology.

6.1.8 Bio-Printing

Bio-printing is one of the fastest-growing areas of three-dimensional printing. The technology uses inkjet-style printers to make living tissue. Using three-dimensional bio-printing for fabricating biological constructs, that typically involve dispensing cells onto a biocompatible scaffold, it uses a successive layer-by-layer approach to generate tissue-like three-dimensional structures; it ensures stability and viability of the cells during the manufacturing process. Some of the methods that are used for three-dimensional bio-printing of cells are photolithography, magnetic bio-printing, stereolithography, and direct cell extrusion.

Benefits: Bio-printing has the potential to be one of the most significant technologies to reduce costs of healthcare in the future. Testing drugs on functional printed human organs could reduce the time to develop and test new drugs in clinical trials. As this technology improves, human organs could be printed in a few hours, rather than relying on donor organs. Examples of bio-printing technologies that could benefit VA healthcare and patients in the future, include printed skin for Veterans who have suffered severe burns, and full-scale human organs and patches that could be used for drug and vaccine testing. While bio-printing may be applicable to the future of healthcare, FDA is likely at least 10 years away from developing bio-printing regulations.

Recommendations: Here are some steps OI&T can take to move forward with existing Bio-Printing efforts:

- Examine guidelines from non-government organizations regarding the cautious use of bio-printing.
- Educate government internal officials, consumers, and the entire agency about the potential benefits and limitations of bio-printing technology.
- Continue to track the FDA’s efforts on bio-printing regulations.³⁹
- Determine if there are other VA needs for additive manufacturing.

6.2 Legal Factors

The US Government has established federal enterprise IT infrastructure statutes, regulations, and guidelines in order to promote advancement and overall efficiency. The statutes and regulations establish policies and requirements to ensure that federal agencies are improving IT infrastructure and driving production. In addition to federal laws, external industry guidance outlines steps and best practices, and OMB guidance and internal VA policies also guide the development of infrastructure. The rapid emergence and evolution of new technologies, capabilities, and best practices, represent major challenges in implementing new or current assets in the IT infrastructure.

While VA is familiar with government statutes, regulations, and guidelines, the content should serve as valuable resources to identify and bridge mission capability gaps in current VA initiatives. Information on how these impact VA’s infrastructure can be found in Appendix B.

7 CONCLUSION

There are several imperatives agreed upon among federal agencies: 1) we need to share common standards and lessons learned by early adopters of technologies; 2) we need to produce better content and data, and present it through multiple channels in a program and device-agnostic manner; 3) we need to adopt a seamless approach to ensure privacy and security in a digital age. While these imperatives are longstanding, many of the solutions are new. Given the realities of a rapidly changing technology landscape, VA must continually evaluate current processes for adopting new technologies and ensuring protection for security and privacy.

³⁹ Additive Manufacturing of Medical Devices: An Interactive Discussion on the Technical Considerations of 3-D Printing; Public Workshop; Request for Comments. FDA Federal Registry Notice. May 14, 2014. <https://www.federalregister.gov/articles/2014/05/19/2014-11513/additive-manufacturing-of-medical-devices-an-interactive-discussion-on-the-technical-considerations>

Currently, the majority of VA's IT environment is characterized as tightly coupled systems that lack a cohesive design and capacity-demand. In addition, numerous duplicative platforms and inefficient processes result in increased costs for O&M for the enterprise. This current state of IT presents VA with significant opportunities for improving the efficiency of current infrastructure in support of successful execution of VA's mission to serve the nation's Veterans. To achieve the future "To Be" IT state of a robust, agile, interoperable infrastructure that offers connectivity, computing capability, and approaches for delivery of integrated services to Veterans, VA will need to move toward a unified IT solutions approach.

There are multiple activities discussed in this document that will enable VA to reach its IT Vision. Enterprise goals of implementing ESS, optimizing IT Infrastructure, and standardizing IT platforms support VA interoperability, agility, reuse, and governance of services, while reducing operational costs. Implementing cloud computing will ensure better use of shared services, enhanced mobile accessibility, and information management. An integrated comprehensive security architecture will protect sensitive Veteran information, regardless of where, how, or when it is accessed. Continuous development of mobile technologies will ensure VA's ability to provide government information anytime, anywhere, and on any device. VA can perform a number of these activities simultaneously, while others will need to be phased-in.

Reaching VA's IT target state will require coordination and cooperation among many leaders in OI&T in order to set and achieve incremental and evolving objectives, competencies, and value measures. Strategic leadership is required to lead the transformation of IT services, obtain consensus on direction and technology investments, ensure efficient execution, and improve strategy management. These efforts will assist OI&T in measuring the attainment of objectives against expected benefits to the business, thereby identifying future infrastructure-related improvements. Achieving VA's IT target state will enable VA to enhance the current mission, shape VA's vision for the future, and present new opportunities to deliver services and benefits.

APPENDIX A: INTERIM IT VISION (3-YEAR)

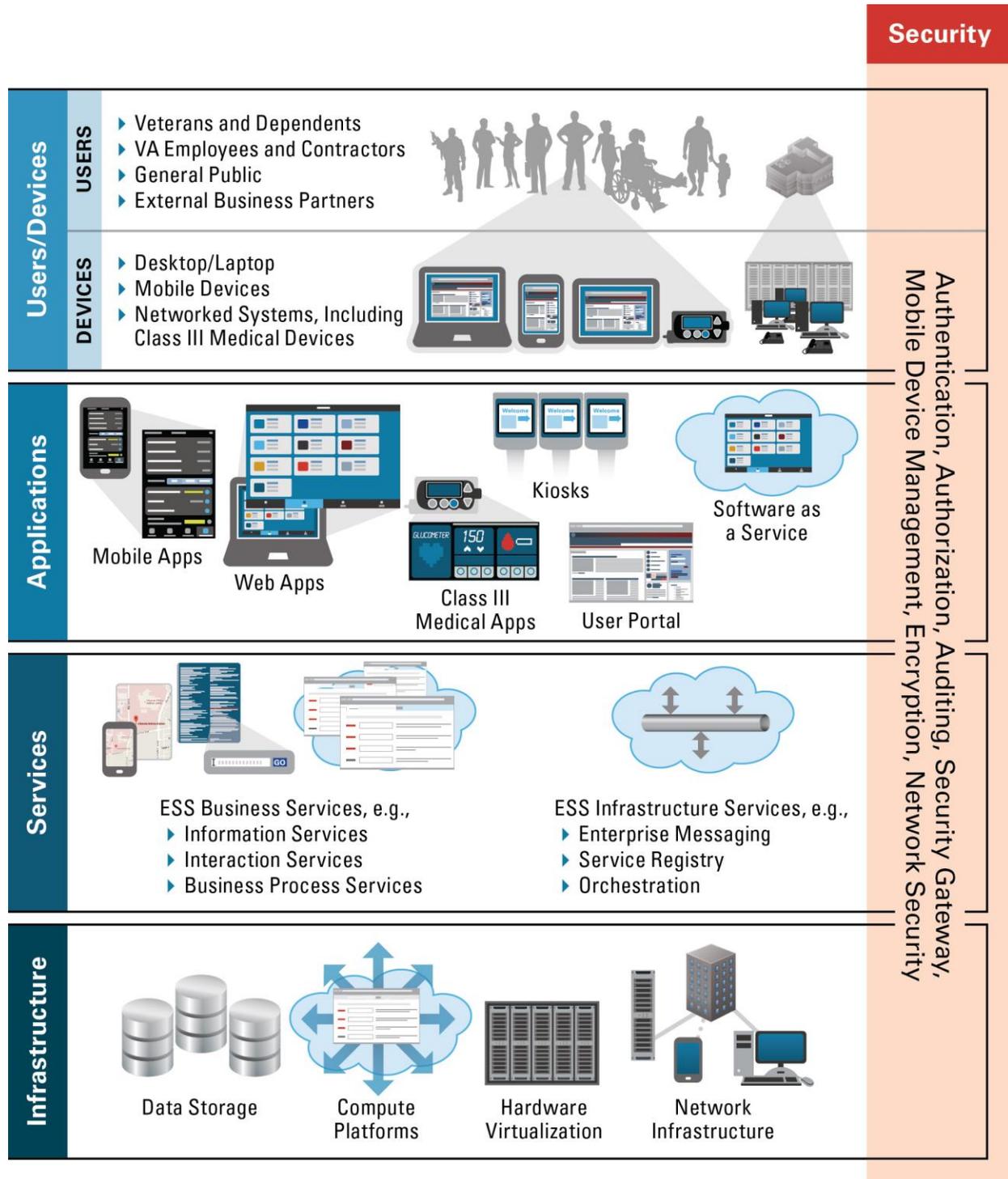


Figure 6: Interim IT Vision (3-Year)

1. USERS/DEVICES:

1.1 Overview: The future vision for IT enables many different ways to access enterprise resources to meet the diverse technology, system, and information needs of a wide range of users and devices. These users include *Veterans and Dependents*, The Department of Veterans Affairs (VA) *Employees and Contractors, General Public, and External Business Partners*, such as the Department of Defense (DoD) (e.g., Defense Health Management System Modernization Health Information Exchange), Veteran Service Organizations, or VA's extended health care network (e.g., Kaiser Permanente, Walgreens) through expansion of the eHealth Exchange and the VA Data Access Service (DAS). These users might choose to access VA resources via various devices including *desktop, laptop, mobile devices, networked systems, including class III medical devices, and external business partner devices*.

Focusing on the end user is a significant driver for meeting business needs, improving the Veteran experience, and ensuring customer and employee satisfaction. A wide range of consumers need to be accommodated, including VHA network of VA Medical Centers (VAMCs) and Community-Based Outpatient Clinics. VA's EHR provided by the Veterans Health Information Systems and Technology Architecture (VistA) is vital to VA's ability to deliver world-class healthcare to Veterans, Service members, and their dependents. The VistA Evolution Program focuses on improvements to VistA to achieve seamless interoperability with other systems (including DoD's EHR) and to improve quality, safety, efficiency, and satisfaction in VA health care using a variety of end-user devices.

VA's goal is to be a world-class customer service organization that provides seamless access to benefits via systems. Interoperability with DoD is progressing with more than 1.5 million data elements⁴⁰ exchanged with the VA each day; however, the DoD is but one important *External Business Partner* for the VA. External business partners include affiliated universities, medical schools, contracted clinics and external providers. Also, Federal agencies such as the Social Security Administration, Department of Education, Housing and Urban Development, and the Department of Justice are included as external business partners.

1.2 Security: VA must ensure that appropriate user-level security measures are implemented to protect the VA's data, systems, and infrastructure. VA will ensure that User Authentication is successfully completed before providing authorized users with access to VA systems, data, or infrastructure. Authentication methods fall into three categories: (1) something the user *knows*, (2) something the user *has*, and (3) something the user *is*. The third factor will include biometrics (e.g., fingerprints, voiceprints, retinal scans), which VA will expand upon in the near-term. Biometrics provide robust multi-factor authentication and mitigate fraudulent activities (e.g., prescription fraud) that pose risks to achieving VA's customer-centric goals.

VA will ensure user-level and device-level security, enforcing VA Handbook 6500. VA Handbook 6500 provides implementation guidance on a standard set of security controls in accordance with NIST SP 800-53 and the FISMA. VA will also enforce the Homeland Security Presidential

⁴⁰ http://www.oit.va.gov/Enabling_Veteran_Health_Care.asp, accessed 15 September 2015.

Directive 12 (HSPD-12), which requires Personal Identity Verification (PIV) credentials and maintenance of a Public Key Infrastructure (PKI) to support users and devices. VA's cybersecurity strategy enables "defense in depth," which provides a holistic security framework that covers the supporting IT infrastructure and networks to the individual user. VA currently provides enterprise-wide security services via an Identity and Access Management (IAM) program and will continue to expand on Single Sign-on (SSO), authorization, and auditing services in the near term to improve the security posture of VA enterprise resources.

2. APPLICATIONS:

2.1 Overview: Applications enable users to interact with VA enterprise resources across a multitude of communications channels. Applications supported by mission-essential IT systems are registered in the VA Systems Inventory. The near-term IT Vision will include enhanced IT Service Management (ITSM) controls to improve efficiencies across VA's IT infrastructure. VA applications leverage a standardized set of modern user interaction capabilities to maximize responsiveness and reduce the processing burden on networks and servers.

Applications support enterprise business needs. New and future application initiatives (e.g., Vets.gov) will be supported by current infrastructure investments and also leverage cloud services. Applications will:

- Support an increasingly mobile workforce and customer base via unified point of service environments (i.e., Veterans Point of Service).
- Improve clinical presentation environments (i.e., Enterprise Health Management Platform).
- Expand mobile platforms (i.e., Connected Health).

Customer-facing initiatives including VA 311 and Veterans Relationship Management (VRM) Customer Relationship Management will deliver enhanced functionality to improve the Veteran experience and VA employee productivity.

The following subsections summarize VA applications to meet mission requirements. Each application will support a variety of product-specific use cases, anticipated capacity needs, and follow VA's standard system development lifecycle governance functions. They will also support:

- Seamless external data sharing to support ongoing initiatives including DoD-VA EHR interoperability.
- Electronic case file transfers.
- Disability questionnaires.
- Compensation and pension exams.
- Integrated care planning coordination.

Mobile Apps: Mobile applications leverage enterprise-wide capabilities for Mobile Device Management (MDM) and Mobile Application Management which include the use of both enterprise application stores for internal applications and external stores for public-facing applications. These applications provide responsive design and can run on a variety of devices

and operating systems (e.g., iOS, Android, Windows Mobile). VA is establishing an enterprise mobile strategy that addresses technology, governance, compliance and security, and support. VA is deploying Enterprise Shared Services (ESS) to support Veteran-facing applications, and VA will expand on them in the next three years. These services include:

- Support for standardized authentication and authorization.
- Scalable, enterprise-wide mobile middleware to support automated Development and Operations (DevOps).
- Standardized analytics.
- Robust internal mobile application store (i.e., integration with third-party stores including Apple App Store and Google Play).

The Mobility Enterprise Design Pattern provides detailed information on the “To Be” architecture principles and constraints for both Veteran-facing and staff-facing devices and applications that leverage these capabilities.

Web Apps: VA is developing applications that consist of dynamic websites using the latest web development standards. These standards include HTML5, Cascading Style Sheets, and JavaScript. While many legacy stand-alone business applications will still be used during the near-term, new green field applications will consist of aggregated back-end data sources and provide a uniform interface for the user. These applications will leverage gateway services that abstract the back-end data sources (i.e., Application Programming Interface (API) gateways) and enable user interaction such that the entire website does not require a full refresh with each action. The (Enterprise Architecture) Service Oriented Architecture (SOA) User Interaction Enterprise Design Pattern provides the architectural framework and constraints for web applications, and requires new applications to use modern development libraries and frameworks as approved through the Technical Reference Model (TRM).

Class III Medical Apps: Class III Medical Applications support critical healthcare decision-making and are subject to Food and Drug Administration (FDA) regulations, including pre-market approval. These applications are distinguishable from other applications due to stringent regulations and different user interfaces. They are also subject to different asset management guidance as they are grouped into medical device enclaves, which are subject to monitoring and control requirements compared to IT assets in regional data centers and hosting environments.

Kiosks: A kiosk provides authorized interaction with VA information in a facility such as a VAMC. Kiosks also will be incorporated in benefits-related scenarios including retrieval of benefit status via regional benefits offices or gravesite location at National Cemeteries.

Software as a Service: Software-as-a-Service (SaaS) applications are hosted and managed by a commercial CSP. SaaS functions include customer relationship management, collaboration, and enterprise resource planning. They provide VA the ability to connect to corporate functions using an external hosting environment. VA’s cloud computing strategy and establishment of an enterprise cloud services broker will enable the Department to incorporate SaaS solutions into the Enterprise Technical Architecture.

User Portal: The portal is a specific type of web application that aggregates information from disparate services and connects them with a common user interface. VA’s enterprise cloud services broker will provide a single interface for acquiring and managing commercial cloud services. My HealthVet and eBenefits represent two prominent examples of public-facing enterprise portals that will evolve and expand functionality to support changing business needs. VA will leverage “thin client” portal solutions that separate application logic from underlying business logic, and prohibit sensitive data from being persisted or transmitted without Federal Information Processing Standard (FIPS) 140-2 cryptographic modules.

Future applications will reduce complexity and enhance scalability to satisfy increasing capacity demands. Applications will leverage ESS that make up the Service layer, and functionality will be decomposed into smaller, loosely coupled units. Full-stack, packaged applications will still be prevalent in the next three years, but these applications will gradually be supplanted by lightweight, heterogeneous applications that are easier to test, deploy, and integrate.

2.2 Security: Applications will integrate with IAM services and leverage Internal and External Authentication capabilities, which includes PIV-only authentication for internal users and a clean separation between end-user device and application Active Directory forests. This will enable enterprise standardization to SSO and integration with ABAC services. External users will be authenticated via other credentials (e.g., student, Veteran, etc.), consuming pre-existing user credentials. Security controls for external network access will continue to evolve, including expansion of security gateways that protect encrypted information going to and from VA’s internal networks.

Mobile security will leverage MDM to provide an encrypted container around mobile applications to prevent data leakage (i.e., app wrapping). MDM will integrate with device registries and policies to ensure version control and that device operating systems are up to date. MDM will use FIPS 140-2 standards to protect data at rest and data in transit.

Applications will leverage security controls to ensure proper confidentiality, integrity, and availability of Personally Identifiable Information (PII) and Protected Health Information (PHI) data. VA’s user authorization processes need to be periodically reviewed and updated to ensure maximization of PII/PHI to authorized users while in compliance with regulatory requirements (e.g., Privacy Act, Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act). VA will stay abreast with future revisions or additions to these regulations and adjust strategic guidance accordingly.

3. SERVICES:

3.1 Overview: The Services layer represents standardized interfaces that provide seamless access to enterprise capabilities such that consuming applications do not need to know the implementation of back-end systems. This allows application developers to concentrate on user experience and business logic, and integrate with services that are consistent with measurable preconditions and expectations. The enterprise direction is to maximize use of reusable services that can be accessed by both internal and external consumers. VA defines these services as ESS using SOA design principles.

ESS will help VA achieve the following goals:

- Advance organizational interoperability and agility through the reuse, interoperability, and governance of services across internal and external organizational and program boundaries.
- Promote the standardization, reuse, interoperability, and composition of the best available capabilities developed under the auspices of any system to meet business and mission requirements.

The near-term strategy for VA is to identify, develop, deploy, and manage a set of ESS that align to business capabilities and strategic drivers. This strategy will help move VA away from system-specific solutions toward enterprise solutions. This shift promotes access to new and existing capabilities as services. It focuses on standardization to facilitate reuse and interoperability among such capabilities. It will help VA resolve recurring challenges to improving and evolving information security, advancing agile interoperability and information sharing, and reducing the total lifecycle cost of IT per the Enterprise Design Patterns Directive (VA Directive 6551).

The ESS roadmap⁴¹ involves achieving enterprise-wide agreement on architecture and governance approaches, and identifying candidate ESS that align to strategic business capabilities characterized in the VA EA and in ASD Product Planning Documents (PPDs). This roadmap also includes plans for SOA infrastructure services over the next 3-5 years to support expanded ESS provisioning, management, and consumption. A summary of the approach for adopting ESS in VA for interoperable data sharing is as follows:

- Phase 1: Establish Governance:
 - Establish the ESS Center of Excellence (ESS-CoE).
 - Gain agreement on governance approaches across lines of business.
- Phase 2: Establish Standards:
 - Establish project-level service design guidelines for ESS architecture, development, and support.
 - Publish ESS implementation guidance and disseminate to project teams.
- Phase 3: ESS Execution:
 - Deploy infrastructure capabilities to support current and projected ESS.
 - Architect, deploy, and sustain ESS in accordance with VA business needs intake and analysis, and PPDs.
 - Support retrofitting of applicable legacy systems to ESS available through VA's SOA infrastructure.
- Phase 4: Continual Improvement:

⁴¹ FY 2013-2015 Enterprise Roadmap Addendum. Department of Veterans Affairs. May 29, 2015. http://www.ea.oit.va.gov/EAOIT/docs/May_2015-Release_Documents/VAFY13-15EnterpriseRoadmapAddendum.pdf

- Update governance processes, standards, and service design guidelines to account for lessons learned.
- Evaluate future state of SOA infrastructure and develop a roadmap for evolving the SOA infrastructure to accommodate emerging technologies.

This approach establishes a framework for mandated ESS following the latest industry standards. The (Enterprise Architecture) Enterprise SOA Design Pattern contains the current list of mandated ESS supporting high-level use cases cutting across healthcare and benefits delivery, and corporate functions including the Corporate Data Warehouse. ESS will be largely autonomous and stateless, and they will require adherence to the following SOA design principles agreed to by the ESS-CoE:

- Encapsulation: Advocates exposing a discrete system capability as an autonomous IT asset (i.e., a service) that can be used by any application that requires the capability.
- Separation of Concerns: Advocates separating different aspects of software system so that each aspect can be developed independently and maintained autonomously.
- Loose Coupling: Advocates reducing dependencies between system components and making the remaining dependencies explicit.
- Business Traceability: Advocates using well-defined heuristics to maintain the “line of sight” from business requirements to the system capabilities that support them.

VA solutions will use a layered architectural framework consistent with the above design principles. This means that applications will not access physical data stores directly, but will use abstracted information services that encapsulate the data stores and enable virtual data access.

ESS Business Services: The Open Group’s SOA Reference Architecture⁴² guides ESS categorization and informs ESS architecture guidance and governance processes for Phases 1 and 2. The ESS-CoE will use the following categories to describe service functionality:

- Interaction: Client-centric services (e.g., portal services) are tied to organizational roles and solution applications.
- Process: Business process services (e.g., workflows) are tied to an organization’s way of doing business. Workflow services will become prevalent as VA goes beyond a Generation 3 EHR in future releases of the VistA Evolution program.
- Business Application: Stand-alone services provide a business-related capability specific to a narrow set of service domains. These services will support specific functions, such as prescription refill or address changes.
- Information: Services (e.g., DAS, data federation services) provide information related to business entities and are broadly used across processes and less specific than process services. These include virtualized data warehouse solutions, and an enterprise “data lake” for both batch and real-time data analytics, as outlined in the (Interoperability and Data Sharing) HDA Enterprise Design Pattern.

⁴² The Open Group, SOA Reference Architecture, ISBN: 1-937218-01-0, November 2011.

- Utility: Stand-alone services provide a discrete, business-related capability, used across a wide range of service domains, and normally have a broad cross-section of stakeholders. This includes testing environments, exposed as service.
- Access: These services (e.g., adapters) provide access to legacy systems and whose service interfaces are tightly coupled to the legacy system interface.
- Partner: These services capture interoperability with partners, isolating VA from changes

ESS will leverage traditional service integration with an Enterprise Service Bus. Legacy service interfaces will continue to use SOAP and Web Service Description Language contracts in the next three years. Increasingly, new service interfaces will be exposed as public-facing Representational State Transfer APIs, using contract-first design and test-driven development principles. VA will also follow new open-source technologies for inter-process communication, such as Thrift, and evaluate its use in enterprise solutions.

The Service Layering and Service Categorization Guideline, which is published on the ESS website, provides detailed implementation guidance on each abstraction layer and service category that informs solution architecture development. Links to related guidance are maintained in (Enterprise Architecture) Enterprise SOA Enterprise Design Pattern.

ESS Infrastructure Services: ESS Infrastructure Services provide the eMI service bus. The eMI is a Commercial Off the Shelf product that supports enterprise message routing and transformation, and includes the WebSphere Registry and Repository (WSRR). Projects will leverage SOA infrastructure platforms using approved technologies and standards captured in the TRM. SOA infrastructure services may also leverage cloud-based services, as explained in the Infrastructure layer.

Infrastructure services also include business rules management, orchestration, event management (e.g., publishing a first notice of death to subscribing systems), and routing to IAM STS. These services also provide end-to-end Application Performance Management (APM), as documented in the (Enterprise Architecture) End-to-End APM Enterprise Design Pattern.

3.2 Security: VA will leverage IAM services to provide a centralized platform for authentication, authorization, and auditing across the Department. Each IAM service will conduct rigorous security assurance testing and will allow external access through security gateway solutions. VA will apply defense in depth to each service by securing system components that comprise the service in accordance with enterprise-wide ITSM techniques and procedures. Privacy Impact Assessments, Privacy Threshold Assessments, and trust boundaries for federated identity services with message-level and transport-level security ensure VA privacy and security. Information services will support archiving consistent with VA and National Archives and Records Administration guidelines and allow for reviewing the provenance of data access for auditing purposes. Exception handling will be applied consistently to each service and will apply an “exception shielding” approach to prevent sensitive information from appearing in audit logs or being seen by the consumer.

4. INFRASTRUCTURE:

4.1 Overview: The Infrastructure layer supports services that are consumed by end users. This infrastructure includes regional data centers and hosting environments for VA systems. The near-term vision for infrastructure involves thorough evaluations of current infrastructure components and determining which components may be reused to meet future business requirements. It involves assessments of existing capabilities and conducting cost-benefit analysis to ascertain their viability as VA shifts to a service-oriented enterprise. VA will leverage private, off-site virtualized environments and commercial CSPs. This will help VA capitalize on the rapid elasticity, on-demand self-service, broad network access, resource pooling, and measured service that they provide to meet growing capacity needs. The following subsections describe different aspects of the infrastructure environment and near-term vision attributes.

Data Storage: Data Storage includes the file systems and hard-drive disks used by applications to store and retrieve information. It constitutes data warehouses and data marts used for both batch and real-time analytics and business intelligence. VA will expand on accessible data storage throughout VA through programs such as VBMS and Chapter 33 Long Term Solution, and will incorporate “big data” technologies such as Hadoop and Spark to support enhanced data analytics and machine learning (to be covered in future Enterprise Design Pattern increments). Storage also ensures that storage area networks in VA’s hosting environments remain in separate tiers from application and web tiers for increased flexibility and security. VA will continue to invest in modern storage systems and applications, and phase out mainframe systems (e.g., Benefits Delivery Network) that present interoperability challenges and tight coupling to legacy business logic.

Compute Platforms: “Compute” harnesses computing power through virtualizing central processing units and memory. VA will evaluate current computing platforms, conduct data center consolidation, and expand virtualization over the next three years in regional data centers. Decoupling storage from computing in the infrastructure enables adaptability and flexibility, and reduces the total cost of operations. Increasingly this is enabled through the use of accredited commercial CSPs managed via an enterprise cloud services broker. This allows VA to trade off costly CapEx with operating expenses, and adapt to rapidly changing requirements. VA will maximize computing power, minimize server sprawl, and ultimately pay for only what it uses.

Hardware Virtualization: Hardware Virtualization focuses on the host environment and infrastructure rather than the computer processing provided. VA leverages virtual machine and hypervisor investments, but will also start looking into operating system-level virtualization containers. Containers are increasingly being used for distributed applications and DevOps. VA will standardize the management of containers throughout the Department. Through the TRM, VA will provide the latest configuration management tools to maximize productivity among developers and operations staff. Hardware virtualization also includes a regular technical refresh strategy, which will allow VA to take advantage of new operating system and application features such as in-memory operations for accelerated performance. New virtualization technologies enable VA to consolidate for significant savings.

Network Infrastructure: The IT vision will be achieved through a robust network infrastructure that includes investments in commercial network providers and IaaS. Enterprise ITSM processes and VA security policies will realize stringent enforcement of Local Area Network (LAN) and Wide Area Network configurations. The near-term vision includes:

- Evolution to software-defined networking and Voice over IP.
- Use of network attached storage through Virtual LANs and subnets using IPv6 addresses.

4.2 Security: The infrastructure will enable full disk-level encryption in accordance with industry standards. The infrastructure includes:

- Outer security controls using Federal Government processes (i.e., EINSTEIN 3, TIC 2.0, continuous monitoring for malicious activity).
- “First line of defense” security gateway consisting of several security components (i.e., firewalls, packet filtering, intrusion detection, data loss prevention, demilitarized zones, decoy systems, end-to-end encryption) used to protect information coming from the public Internet.
- Mobile security through the use of MDM.
- Hierarchy of trust through a robust PKI and Non-Personal Entry security controls.

The near-term vision also includes the use of approved trusted platform modules, host-based security packages, and patch management for hosts and servers. ITSM processes will manage these certificates and other configuration items using automated vulnerability scanning, dependency mapping, and federated configuration management system. Data centers and servers will be subject to the same asset and configuration management processes.

USE CASES

Users	Devices	Description
Veterans/ Dependents	Desktop / Laptop	User: Veterans/ Dependents and VA employees/ contractors accessing VA resources via a personal (non-VA issued) Desktop/ Laptop computer. <ul style="list-style-type: none"> • Users shall have the same procedure to login to access resources regardless of reason for access.
Veterans/ Dependents	Mobile Device	User: Veterans/ Dependents and VA employees/ contractors accessing VA resources via a personal (non-VA issued) mobile device. <ul style="list-style-type: none"> • Users shall have the same procedure to login to access resources regardless of reason for access.
Veterans/ Dependents	Networked Systems, including Class III Medical Apps	N/A
VA Employees/ Contractors	Desktop / Laptop	User: VA employees/ contractors accessing VA resources via VA issued desktop or laptop. <ul style="list-style-type: none"> • Users shall have the same procedure to login to access resources regardless of reason for access.
VA Employees/ Contractors	Mobile Device	User: VA employees/ contractors accessing VA resources via a VA issued mobile device. <ul style="list-style-type: none"> • Users shall have the same procedure to login to access resources regardless of reason for access.
VA Employees/ Contractors	Networked Systems, including Class III Medical Apps	User: VA employees accessing and/or creating patient data via Class III Medical Devices or Apps.
General Public	Desktop / Laptop	User: General public accessing VA resources via a desktop device.
General Public	Mobile Device	User: General public accessing VA resources via a mobile device.
General Public	Networked Systems, including Class III Medical Apps	N/A
External Business Partner	Desktop / Laptop	User: External business partner accessing VA resources via a personal (non-VA issued) Desktop/ Laptop computer. <ul style="list-style-type: none"> • Users shall have the same procedure to login to access resources regardless of reason for access.
External Business Partner	Mobile Device	User: External business partner accessing VA resources via a personal (non-VA issued) mobile device.

		<ul style="list-style-type: none"> • Users shall have the same procedure to login to access resources regardless of reason for access.
External Business Partner	Networked Systems, including Class III Medical Apps	<p>User: External business partner accessing VA enterprise resources via networked system exchange.</p> <ul style="list-style-type: none"> • Communication between VA and the Business Partner may require high bandwidth circuits or pass large volumes of data.

USERS:

- **Veterans/ Dependents:** Any individual user accessing Department of Veterans Affairs (VA) systems with VA issued Veteran or Service Member credentials (e.g., Veterans, service members, family members of veterans or service members, and caregivers accessing Veteran or service member records).
- **VA Employees/ Contractors:** Any individual user accessing VA systems with VA issued employee credentials (e.g., direct VA employees and contractors at medical facilities, clinics, and administrative and benefits offices).
- **General Public:** Any individual user accessing VA resources without any previously issued credentials.
- **External Business Partner:** A non-VA business organization that has a pre-established relationship with VA, often involving an agreement regarding exchange of information between the External Business and VA systems (e.g., affiliated universities, contracted clinics, medical schools, and other government agencies such as DoD medical treatment facilities).

DEVICES:

- **Desktop/ Laptop:** A desktop or laptop computer. Term is used to contrast with a mobile or handheld device. Can be VA issued or personal.
- **Mobile Device:** A portable handheld computing device (e.g., smart phone, tablet). Can be VA issued or personal.
- **Networked Systems, including Class III Medical Applications (Apps):**
 - Networked systems are a group of two or more systems linked together to share information or services. Can be VA or External Business Partner systems.
 - Class III Medical Devices are generally the highest risk devices, as classified by the FDA based on the level of control necessary to assure safety and effectiveness. Class III devices are usually those that support or sustain human life or are of substantial importance in preventing impairment of human health and must typically be approved by FDA before they are marketed (e.g., implantable pacemaker, pulse generators, HIV diagnostic tests, and automated external defibrillators). Class III Medical Devices are connected to VA network and used to support medical diagnosis and treatment. They are used only by authorized VA staff (i.e., licensed practitioners). Medical devices are tracked through special asset management procedures for medical devices.

APPENDIX B: STATUTORY, REGULATORY AND GUIDANCE FACTORS

Statutes Name	Statutes Description	Impact to VA
The Government Performance Results Modernization Act	The Government Performance Results Modernization (GPRA Modernization) Act is an update on the GPRA that required agencies to publish performance improvement activities (i.e., setting goals, measuring results, reporting progress, etc.) in machine-readable formats, ultimately allowing agencies to view each other's practices. ⁴³	VA publishes performance and strategic planning documentation to assess past and current performance to shape future vision as an enterprise. These activities help innovate VA's IT infrastructure to keep it moving forward from an IT perspective.
The Health Information Technology for Economic and Clinical Health Act	The Health Information Technology for Economic and Clinical Health Act is a portion of The American Recovery and Reinvestment Act that pertains to increasing the use of EHR by physicians and hospitals. ⁴⁴	With VA focused on achieving meaningful use of Health IT, there is potential to increase the abilities of the VistA. HealtheVet ⁴⁵ is the next generation of VistA, offering advanced capabilities and flexibility to adapt to healthcare and technology innovation for continuous improvement of Veteran healthcare.
The E-Government Act	The E-Government (E-Gov) Act was created to improve the management and promotion of electronic government services and processes to improve citizens' access to information and services. ⁴⁶	With VA focused on providing health services anywhere/anytime, the need to determine cyberspace performance metrics, standards and policies, to ensure that sensitive electronic information of patients is handled accordingly, is imperative.
Capital Planning and Investment Control	Capital Planning and Investment Control (CPIC) is a management process for the ongoing identification, selection, control, and evaluation of IT investments within agencies as mandated within the reporting requirements of the Clinger-Cohen Act. ⁴⁷	Maximizing capital investment of IT resources is extremely important to VA, in order to bring the highest quality of information management to the department and its Veterans as well as properly implement spending throughout the VA's IT infrastructure.

⁴³ Government Performance and Results Modernization Act. U.S. Government Publishing Office. January 4, 2011. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ352/pdf/PLAW-111publ352.pdf>

⁴⁴ About the HITECH Act. HITECH Answers. 2015. <http://www.hitechanswers.net/about/about-the-hitech-act-of-2009/>

⁴⁵ eHEALTH: VistA. US Department of Veterans Affairs. June 23, 2015. <http://www.ehealth.va.gov/VistA.asp>

⁴⁶ E-Government Act of 2002. Wikipedia. July 20, 2014. http://en.wikipedia.org/wiki/E-Government_Act_of_2002

⁴⁷ Management of Federal Information Resources. US Office of Management and Budget. http://www.whitehouse.gov/omb/fedreg_a130notice/

<p>Clinger-Cohen Act</p>	<p>The Clinger-Cohen Act is designed to supplement IT resource management polices by establishing a comprehensive approach for agencies to improve the acquisition and management of IT resources; mainly through resource planning, CPIC processes, and rethinking work streams before IT investments.</p>	<p>VA must focus on staying up-to-date with the most current technologies that will impact information management as the amount of Veterans and information is constantly growing. Being able to manage cost as well as provide the most efficient information management is essential to VA and its Veterans.</p>
<p>Government Management Reform Act</p>	<p>The Government Management Reform Act (GMRA) provides a more effective, efficient, and responsive government through a series of management reforms primarily for federal human resources and financial management. The Act requires agencies to prepare a financial statement covering all accounts and associated activities of the agency.⁴⁸</p>	<p>VA is required to prepare financial statements to reflect overall financial position, to ensure that the agency’s finances are being implemented properly and the results are efficient. Maximizing VA’s return on every tax dollar is highly important to VA, the government and Veterans.</p>
<p>The Telework Enhancement Act</p>	<p>The Telework Enhancement Act (Public Law 111-292) provides a framework of requirements for federal agencies to leverage teleworking as an asset to the enterprise.⁴⁹</p>	<p>VA is able to establish a teleworking policy (that abides by requirements of the Act) that will provide opportunities to reduce costs of office spaces and traveling as well as take full advantage of IT as a service.</p>
<p>Veterans Access, Choice and Accountability Act</p>	<p>The Veterans Access, Choice and Accountability Act (VACAA) aims to improve the access to and quality of care for Veterans, provide real accountability for senior managers, and improve education benefits for Veterans and their dependents.</p>	<p>VACAA requires the evaluation of VA healthcare and its access, as well as provides authorization to eligible Veterans to receive non-VA care. Might lead to additional instances of information exchange with external service providers of healthcare and education.</p>

⁴⁸ Authorities Under Which the OIG Carries Out Its Work. US Department of Labor.

<http://www.oig.dol.gov/statutory.htm#gmra>

⁴⁹ Guidance for Federal Agencies. Telework.gov.

http://www.telework.gov/Telework_Enhancement_Act/Guidance/index.aspx#General

<p>OMB Circular A-11, Part 7: Planning, Budgeting, Acquisition, and Management of Capital Assets</p>	<p>Part 7 of Circular A-11 establishes policy for planning, budgeting, acquisition, and management of federal capital assets, as well as instructs agencies on budget justification and reporting requirements for major IT investments and for major non-IT capital assets.⁵⁰</p>	<p>A-11 requires VA to reduce spending on lower priority programs in order to create room for effective investments in areas critical to its mission. This includes planning for IT investments to gain efficiencies such as consolidating computing, applications and networks.</p>
<p>OMB Memorandum M-06-02: Public Access and Dissemination of Government Information</p>	<p>This memorandum identifies required procedures to organize and categorize information and make it searchable across agencies to improve public access and dissemination. It requires agencies to use the Federal Enterprise DRM or justify deviances within their enterprise architecture.⁵¹</p>	<p>VA has a wide array of information ranging from Veterans’ personal data and health records to general VA information. VA is required to disseminate information properly within VA and among agencies, as well as make specific information publically accessible to promote service efficiency and quality, all while ensuring its security.</p>
<p>OMB Circular A-130: Management of Federal Information Resources</p>	<p>Circular A-130 establishes policy for the management of information resources across the federal government to meet information management requirements, which ultimately promotes the dissemination of government information among agencies.⁵²</p>	<p>VA is required to have a management process for ongoing identification, selection, control, and evaluation of investments in information resources that align with its strategic missions. It also outlines how VA is to use, share and protect public information.</p>
<p>OMB Digital Government Strategy</p>	<p>The Digital Government Strategy aims to leverage current and emerging technologies to successfully deliver high-quality digital government information and services anywhere, anytime, and on any device.⁵³</p>	<p>With the advancement of mobile technology and applications VA will need to move towards a more agile, client-centric environment, providing Veterans with VA information and services anytime, anywhere, and on any device.</p>

⁵⁰ Office of Management and Budget, Circular No. A-11, Part 7: Planning, Budgeting, Acquisition, and Management of Capital Assets. Whitehouse.gov. June 2008.

https://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/a_11_2008.pdf

⁵¹ OMB Memorandum M-06-02. Whitehouse.gov. December 16, 2005.

<https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-02.pdf>

⁵² OMB Circular A-130. Wikipedia. December 20, 2014. http://en.wikipedia.org/wiki/OMB_Circular_A-130#cite_note-A130Initial-1

⁵³ Digital Government. Office and Management and Budget.

<http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html>

<p>OMB IT Shared Services Strategy</p>	<p>The IT Shared Services Strategy (“Shared-First Strategy”) provides guidance to federal agencies through policies on the full range and lifecycle of intra- and inter-agency IT shared services, which will enable the implementation of IT functions that can be consumed by multiple organizations within or between agencies.⁵⁴</p>	<p>Leveraging IT shared services will allow multiple organizations within VA to take advantage of specific IT functions (i.e., data storage, generation, processing, etc.) from one source rather than using multiple systems allocated to different VA organizations, thus eliminating redundancies and reducing investment and maintenance costs.</p>
<p>OMB Federal CIO 25-Point IT Reform Action Plan</p>	<p>This Action Plan details 25 steps federal agencies must take to reform the way they use IT assets to combat the pervasive inefficiencies and expenses of agencies IT infrastructure, and move towards a more nimble and citizen-focused future.⁵⁵</p>	<p>Constant reformation and innovation of IT assets within VA is essential, not only to cut cost and improve efficiency, but to explore and pave the way for the implementation of new IT capabilities that can benefit VA’s employees and Veterans.</p>
<p>OMB Cloud First Policy</p>	<p>The Cloud First Policy mandates that all federal agencies take advantage of cloud computing to improve IT flexibility, maximize IT capabilities and agility, and minimize cost.⁵⁶</p>	<p>Cloud computing is the glue that will enable VA to transition to a more client-centric environment, fully integrating the essentials of a modernized IT infrastructure, and take full advantage of IT innovation to better serve Veterans.</p>
<p>OMB IPv6 Transition Guidance</p>	<p>This memorandum describes the steps to transition to the next IP, version 6 (IPv6), which is intended to have improved scalability, simplicity, and security over legacy protocol, to meet the demands of key federal IT initiatives.⁵⁷</p>	<p>VA created the VA IPv6 Transition Plan to provide guidance aligned with the VA EA, VA Capital Planning policies and procedures, and OMB directives, to stakeholders responsible for the development of the transition to IPv6.⁵⁸</p>

⁵⁴ Federal Information Technology Shared Services Strategy. Office of Management and Budget. May 2, 2012. https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/shared_services_strategy.pdf

⁵⁵ 25 Point Implementation Plan to Reform Federal Information Technology Management. US Chief Information Officer. December 9, 2010. <https://cio.gov/wp-content/uploads/downloads/2012/09/25-Point-Implementation-Plan-to-Reform-Federal-IT.pdf>

⁵⁶ Cloud IT Services. US General Services Administration. August 18, 2015. <http://www.gsa.gov/portal/content/190333>

⁵⁷ Memorandum on the Transition to IPv6. Office of Management and Budget. September 28, 2010. https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/transition-to-ipv6.pdf

⁵⁸ Department of Veterans Affairs Enterprise Architecture Guidance for the VA IPv6 Network Transition. VA Enterprise Architecture. January 12, 2006. http://www.hpc.mil/images/hpcdocs/ipv6/va_guidance_for_ipv6_transition.pdf

<p>OMB Federal Data Center Consolidation Initiative (FDCCI)</p>	<p>The OMB Federal Data Center Consolidation Initiative (FDCCI) aims to assist agencies in the consolidation of data centers to address green initiatives, reduce costs, and shift IT investment to more efficient computing platforms and technologies.⁵⁹</p>	<p>Aggressive pursuance in consolidating data centers enables VA to reduce costs and environmental impact, while improving efficiency and quality of IT services provided to Veterans and employees.⁶⁰</p>
<p>Homeland Security Presidential Directive</p>	<p>The Homeland Security Presidential Directive (HSPD-12) establishes a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to employees and contractors for access to federally-controlled facilities and networks.⁶¹</p>	<p>VA possesses sensitive personal information and health records of both employees and Veterans, which are essential to keep secure. Providing regulated and restricted access to VA networks and facilities is the first step to keep sensitive information safe.</p>

⁵⁹ FDCCI FAQs. US Chief Information Officer. May 2012. <https://cio.gov/wp-content/uploads/downloads/2012/09/FAQ-May-2012-Update-V1.pdf>

⁶⁰ FDCCI VA 2011 Data Center Consolidation Plan and Progress Report. US Chief Information Officer. September 30, 2011. http://www.hpc.mil/images/hpcdocs/ipv6/va_guidance_for_ipv6_transition.pdf

⁶¹ Homeland Security Presidential Directive (HSPD) 12. US Department of Agriculture. June 2, 2015. <https://hspd12.usda.gov/about.html>

APPENDIX C: BIBLIOGRAPHY

Reference Number	Reference (Title. Source. Date. Link)
1	Memorandum: VA Regional Alignment. Department of Veterans Affairs Chief of Staff. January 26, 2015. http://afgenvac.org/wp-content/uploads/2015/01/VA-Regional-Alignment-Memo-Single-VA-Website-Memo.pdf
2	FY 2013-2015 Enterprise Roadmap Addendum. Department of Veterans Affairs. May 29, 2015. http://www.ea.oit.va.gov/EAOIT/docs/May_2015-Release_Documents/VAFY13-15EnterpriseRoadmapAddendum.pdf
3	FY 2013-2015 Enterprise Roadmap Addendum. Department of Veterans Affairs. May 29, 2015.
4	OI&T Enterprise Strategy Town Hall. Department of Veterans Affairs. October 21, 2015.
5	2014 Performance and Accountability Report. Department of Veterans Affairs. November 17, 2014. http://www.va.gov/budget/docs/report/2014-VAparFullWeb.pdf
6	Veterans Statistics – Veterans Day 2015. US Census. November 11, 2015. http://www.census.gov/library/infographics/veterans-statistics.html
7	Congressional Submission for FY2016 Funding and FY2017 Advanced Appropriations. Department of Veterans Affairs. http://www.va.gov/budget/docs/summary/Fy2016-Volumell-MedicalProgramsAndInformationTechnology.pdf
8	VA Handbook 6500. Department of Veterans’ Affairs. March 2015. http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=793&FType=2
9	(Mobility) Mobile Architecture V2.0 Enterprise Design Pattern. Department of Veteran’s Affairs. http://www.techstrategies.oit.va.gov/docs_design_patterns.asp
10	FY 2013-2015 Enterprise Roadmap, Department of Veterans Affairs. March 28, 2014. http://www.ea.oit.va.gov/docs/VA_Enterprise_Roadmap_2_FINAL_20140409.pdf
11	(Interoperability and Data Sharing) Hybrid Data Access Enterprise Design Pattern. December 28, 2015.
12	Homeland Security Presidential Directive (HSPD) 12. Department of Agriculture. June 2, 2015. https://hspd12.usda.gov/about.html
13	CIO Annual Report. Department of Veterans Affairs. 2013 (Draft).
14	Office of Information Security (OIS) Overview. Department of Veterans Affairs. http://www.ois.oit.va.gov/OIS_Overview.asp
15	VA Dashboard. Department of Veterans Affairs. http://dashboard.tic.va.gov/s/ST/
16	2014 Performance and Accountability Report. Department of Veterans Affairs. November 17, 2014. http://www.va.gov/budget/docs/report/2014-VAparFullWeb.pdf
17	FY 2013-15 Information Resource Management Strategic Plan. Department of Veterans Affairs. March 28, 2014. http://www.ea.oit.va.gov/EAOIT/docs/VA_IRM_Strategic_Plan_Final_Signed_20140424.pdf
18	(Enterprise Architecture) SOA - VistA Evolution Enterprise Design Pattern. Department of Veterans’ Affairs. http://www.techstrategies.oit.va.gov/docs_design_patterns.asp
19	Vista Evolution Program Plan. Department of Veteran’s Affairs. March 2014. https://www.osehra.org/sites/default/files/vista_evolution_program_plan_3-24-14.pdf
20	CIO Annual Report. Department of Veterans Affairs. 2013 (Draft).
21	Digital Government Strategy. The White House. May 23, 2012. https://eapad.dk/gov/us/digital-government-strategy/
22	Information Security Webinar Series: Mobile Device Security. The Department of Veterans Affairs. December 14, 2015.
23	VA Launches Open Source Custodian. Veterans Today. August 30, 2011. http://www.veteranstoday.com/2011/08/30/va-launches-open-source-custodian/
24	The Open Government Partnership, National Action Plan for the United States. The White House.

Reference Number	Reference (Title. Source. Date. Link)
	September 20, 2011. http://www.whitehouse.gov/sites/default/files/us_national_action_plan_final_2.pdf
25	Memorandum: Consideration of Open Source Software. Department of Veterans Affairs CIO. Nov 4, 2014. http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=804&FType=2
26	CIO Annual Report. Department of Veterans Affairs. 2013 (Draft).
27	Federal Data Center Consolidation Initiative. Office of Management and Budget. February 26, 2010. https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal_data_center_consolidation_initiative_02-26-2010.pdf
28	RRTF Common News Newsletter. Department of Veterans Affairs. May 2015. http://vaww.blog.va.gov/rrtf/wp-admin/post-new.php#_ftn1
29	OMB Circular A-130. Wikipedia. December 20, 2014. http://en.wikipedia.org/wiki/OMB_Circular_A-130#cite_note-A130Initial-1
30	CIO Annual Report. Department of Veterans Affairs. 2013 (Draft).
31	A Simple Explanation of 'The Internet of Things'. Forbes. May 13, 2014. http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/
32	A Simple Explanation of 'The Internet of Things'. Forbes. May 13, 2014. http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/
33	An Introduction to the Internet of Things (IoT). Cisco. November 2013. http://www.cisco.com/web/solutions/trends/iot/introduction_to_IoT_november.pdf
34	Cognizant: Reaping the Benefits of the Internet of Things. Cognizant. May 2014. http://www.cognizant.com/InsightsWhitepapers/Reaping-the-Benefits-of-the-Internet-of-Things.pdf
35	A New Style Is Emerging in the Enterprise: Software-Defined Architecture. InfoQ. May 24, 2014. http://www.infoq.com/news/2014/05/sda?utm_reader=feedly
36	Securing Mobile Healthcare Devices: Best Practices. InformationWeek. June 3, 2014. http://www.informationweek.com/healthcare/security-and-privacy/securing-mobile-healthcare-devices-best-practices/d/d-id/1269357
37	Five steps organizations can take to manage mobile devices used by health care providers and professionals. HealthIT.gov. January 15, 2013. http://www.healthit.gov/providers-professionals/five-steps-organizations-can-take-manage-mobile-devices-used-health-care-pro
38	Mobile Devices and Apps for Health Care Professionals: Uses and Benefits. National Institutes of Health. May 2014. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4029126/
39	Additive Manufacturing of Medical Devices: An Interactive Discussion on the Technical Considerations of 3-D Printing; Public Workshop; Request for Comments. FDA Federal Registry Notice. May 14, 2014. https://www.federalregister.gov/articles/2014/05/19/2014-11513/additive-manufacturing-of-medical-devices-an-interactive-discussion-on-the-technical-considerations
40	http://www.oit.va.gov/Enabling_Veteran_Health_Care.asp , accessed 15 September 2015.
41	FY 2013-2015 Enterprise Roadmap Addendum. Department of Veterans Affairs. May 29, 2015. http://www.ea.oit.va.gov/EAOIT/docs/May_2015-Release_Documents/VAFY13-15EnterpriseRoadmapAddendum.pdf
42	The Open Group, SOA Reference Architecture, ISBN: 1-937218-01-0, November 2011.
43	Government Performance and Results Modernization Act. U.S. Government Publishing Office. January 4, 2011. http://www.gpo.gov/fdsys/pkg/PLAW-111publ352/pdf/PLAW-111publ352.pdf
44	About the HITECH Act. HITECH Answers. 2015. http://www.hitechanswers.net/about/about-the-

Reference Number	Reference (Title. Source. Date. Link)
	hitech-act-of-2009/
45	eHEALTH: VistA. US Department of Veterans Affairs. June 23, 2015. http://www.ehealth.va.gov/VistA.asp
46	E-Government Act of 2002. Wikipedia. July 20, 2014. http://en.wikipedia.org/wiki/E-Government_Act_of_2002
47	Management of Federal Information Resources. US Office of Management and Budget. http://www.whitehouse.gov/omb/fedreg_a130notice/
48	Authorities Under Which the OIG Carries Out Its Work. US Department of Labor. http://www.oig.dol.gov/statutory.htm#gmra
49	Guidance for Federal Agencies. Telework.gov. http://www.telework.gov/Telework_Enhancement_Act/Guidance/index.aspx#General
50	Office of Management and Budget, Circular No. A-11, Part 7: Planning, Budgeting, Acquisition, and Management of Capital Assets. Whitehouse.gov. June 2008. https://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/a_11_2008.pdf
51	OMB Memorandum M-06-02. Whitehouse.gov. December 16, 2005. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-02.pdf
52	OMB Circular A-130. Wikipedia. December 20, 2014. http://en.wikipedia.org/wiki/OMB_Circular_A-130#cite_note-A130Initial-1
53	Digital Government. Office and Management and Budget. http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html
54	Federal Information Technology Shared Services Strategy. Office of Management and Budget. May 2, 2012. https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/shared_services_strategy.pdf
55	25 Point Implementation Plan to Reform Federal Information Technology Management. US Chief Information Officer. December 9, 2010. https://cio.gov/wp-content/uploads/downloads/2012/09/25-Point-Implementation-Plan-to-Reform-Federal-IT.pdf
56	Cloud IT Services. US General Services Administration. August 18, 2015. http://www.gsa.gov/portal/content/190333
57	Memorandum on the Transition to IPv6. Office of Management and Budget. September 28, 2010. https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/transition-to-ipv6.pdf
58	Department of Veterans Affairs Enterprise Architecture Guidance for the VA IPv6 Network Transition. VA Enterprise Architecture. January 12, 2006. http://www.hpc.mil/images/hpcdocs/ipv6/va_guidance_for_ipv6_transition.pdf
59	FDCCI FAQs. US Chief Information Officer. May 2012. https://cio.gov/wp-content/uploads/downloads/2012/09/FAQ-May-2012-Update-V1.pdf
60	FDCCI VA 2011 Data Center Consolidation Plan and Progress Report. US Chief Information Officer. September 30, 2011. http://www.hpc.mil/images/hpcdocs/ipv6/va_guidance_for_ipv6_transition.pdf
61	Homeland Security Presidential Directive (HSPD) 12. US Department of Agriculture. June 2, 2015. https://hspd12.usda.gov/about.html

APPENDIX D: ACRONYMS

Acronym	Definition
ABAC	Attribute-based Access Control
ADS	Authoritative Data Sources
AERB	Architecture and Engineering Review Board
AITC	Austin Information Technology Center
AoA	Analysis of Alternatives
API	Application Programming Interface
APM	Application Performance Management
ASD	Office of Architecture, Strategy, and Design
BHIE	Bidirectional Health Information Exchange
BISL	Business Intelligence Service Line
BYOD	Bring Your Own Device
CapEx	Capital Expenses
CBOC	Community-based Outpatient Clinics
CCD	Common Customer Data
CIO	Chief Information Officer
CMDB	Configuration Management Database
COTS	Commercial-off-the-shelf
CPIC	Capital Planning and Investment Control
CRISP	Continuous Readiness in Security Program
CSP	Cloud Service Provider
DAS	Data Access Services
DevOps	Development and Operations
DoD	Department of Defense
EA	Enterprise Architecture
EAC	Enterprise Architecture Council
EAWG	Enterprise Architecture Working Group
eCRUD	Enterprise Create, Read, Update Delete
EDE	Enterprise Development Environment
EHR	Electronic Health Records
ELA	Enterprise-Level Agreement
ELDM	Enterprise Logical Data Model
EMF	Enterprise Management Framework
eMI	Enterprise Messaging Infrastructure
EMM	Enterprise Mobility Management
ESS	Enterprise Shared Services
ESS-CoE	Enterprise Shared Services Center of Excellence
ETA	Enterprise Technical Architecture
ETAWG	Enterprise Technical Architecture Working Group
ETSP	Enterprise Technology Strategic Plan
FCCX	Federal Cloud Credential Exchange
FDA	Food and Drug Administration
FDCCI	Federal Data Center Consolidation Initiative
FDR	Federated Data Repository
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act

Acronym	Definition
FY	Fiscal Year
GFE	Government-furnished Equipment
GMRA	Government Management Reform Act
GO/CO	Government Owned and Contractor Operated
GOTS	Government-off-the-Shelf
GPRA	Government Performance Results Act
GUI	Graphical User Interface
HDA	Hybrid Data Access
HSPD	Homeland Security Presidential Directive
IaaS	Infrastructure-as-a-Service
IAM	Identity and Access Management
IOC	Initial Operating Capability
IoT	Internet of Things
IP	Internet Protocol
IRM	Information Resources Management
IT	Information Technology
ITSM	Information Technology Service Management
LAN	Local Area Network
LOA	Level of Authority
MAM	Mobile Application Management
MDM	Mobile Device Management
MDR	Managed Data Repositories
MGD	Machine-generated Data
MVI	Master Veteran Index
NCPS	National Cybersecurity Protection System
NIST	National Institute of Standards and Technology
NoSQL	Non-Structured Query Language
NPE	Non-Personal Entry
NSD	National Service Desk
NSOC	Network and Security Operations Center
O&M	Operations & Maintenance
OCA	Operational Capabilities Assessment
OI&T	Office of Information & Technology
OIS	Office of Information Security
OMB	Office of Management and Budget
OpEx	Operational Expense
OSEHRA	Open Source Electronic Health Record Alliance
OSS	Open Source Software
PaaS	Platform-as-a-Service
PACS	Physical Access Control Systems
PBX	Private Branch Exchange
PD	Office of Product Development
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PMAS	Project Management and Accountability System

Acronym	Definition
POPT	Privacy Officer Professionalization Training
PPD	Product Planning Documents
PTA	Privacy Threshold Analysis
RPC	Remote Procedure Call
RRTF	Ruthless Reduction Task Force
SaaS	Software-as-a-Service
SDE	Office of Service Delivery and Engineering
SDN	Software Defined Networking
SOA	Service Oriented Architecture
SORN	Systems of Record Notice
SQL	Structured Query Language
SSO	Single Sign-on
STS	Secure Token Service
TAC	Technology Acquisition Center
TIC	Trusted Internet Connection
TRM	Technical Reference Model
TS	Office of Technology Strategies
V2E	Visibility to Everything
VA	Department of Veterans Affairs
VaaS	Voice-as-a-Service
VACAA	Veterans Access, Choice, and Accountability Act
VACO	Department of Veterans Affairs Central Office
VAMC	VA Medical Center
VA EA	VA Enterprise Architecture
VBMS	Veterans Benefits Management System
VHA	Veterans Health Administration
VIP	Veteran-focused Integration Process
VistA	Veterans Health Information Systems and Technology Architecture