U.S. Department of Veterans Affairs
IT Governance Structure

Office of Information & Technology

May 23, 2012

CONTENTS

List of Figures

List of Tables

U.S. Department of Veterans Affairs
IT Governance Structure

1. PURPOSE

This document provides a summary of the Department of Veterans Affairs' (VA) approach to information technology (IT) governance. Its contents, along with associated documentation, include the governance structure's defined scope of authority, core principles to guide action, and established roles and responsibilities.

2. CORE PRINCIPLES

The core principles are embodied in VA's continued focus on advancing toward the strategic goals established to transform VA into an innovative, 21st century organization that is people-centric, results-driven, and forward looking. Critical to this achievement is customer service and a cooperative approach among the Office of Information and Technology, VA's Administrations (Veterans Health, Veterans Benefits, and National Cemeteries), and corporate staff offices. It is in this spirit that information technology proudly supports our strategic goals as we rapidly deliver technology to transform VA.

3. BACKGROUND

IT plays a pivotal role in the transformation of VA into a 21st century organization as envisioned by the President and Secretary Shinseki. IT is an enabler for implementation of the Secretary's 16 Transformational Initiatives, which cannot be executed without newly developed IT products. These initiatives are key to improving VA's service to Veterans.

The VA IT enterprise is a massive single, consolidated network with 152 hospitals, 791 community-based outpatient clinics (CBOC), 57 benefits processing offices, and 131 cemeteries and 33 soldier's lots and monument sites. Our OIT workforce numbers over 7,100, serving over 300,000 VA employees and more than 10 million Veterans. Within our $3.1 billion FY 2011 budget, OIT manages a technology profile of over 314,000 desktop computers, 30,000 laptops, 18,000 blackberries and mobile devices, and 448,000 email accounts. These figures describe an IT enterprise that is one of the largest consolidated IT organizations in the world. Managing an organization of this size and scope requires disciplined management and processes. Various IT governance bodies exist to address business requirements, planning, prioritization, resourcing, and technical aspects of information technology.

Effective information technology governance enables centralized decision-making to address business needs and align IT strategy, systems, services, and processes to the Department's strategic goals. Appropriate information technology governance in concert with a tone of cooperation among the VA stakeholders has made and will continue to make it possible to effectively address many complex problems and issues at the second largest agency in the Federal Government.

4. VA IT GOVERNANCE STRUCTURE

Key IT governance bodies within VA include the following:

- 3 Boards
    1. **Information Technology Leadership Board** (ITLB) – serves as the senior level IT governance board.
    2. **Planning, Programming, Budget Execution Board** (PPBEB) - focuses on budget formulation and execution; coordinates the development of the IT Multi-Year Program; and facilitates the programming process for IT investments.
    3. **Architecture and Engineering Review Board** (AERB) – facilitates the development, validation, publication, and maintenance of enterprise architecture policies, standards, procedures, and artifacts.
- 2 Councils
    1. **Enterprise Architecture Council** (EAC) – serves as oversight body for VA's enterprise architecture.
    2. **Data Governance Council** (DGC) – oversees data governance policy, authoritative data sources, data architecture, and master data management.
- 1 Committee
    1. **Integrated Steering Committee** (ISC) – supports integration across major initiatives in VA.

VA's IT governing bodies assist in setting the conditions for success, and facilitate effective IT governance and executive decision making. They serve to improve the accountability and effectiveness of the expenditure of resources to provide IT solutions, systems, products, and services. The figure below illustrates the VA IT Governance Structure. It is followed by a table outlining the roles and responsibilities of each of VA's governing bodies.

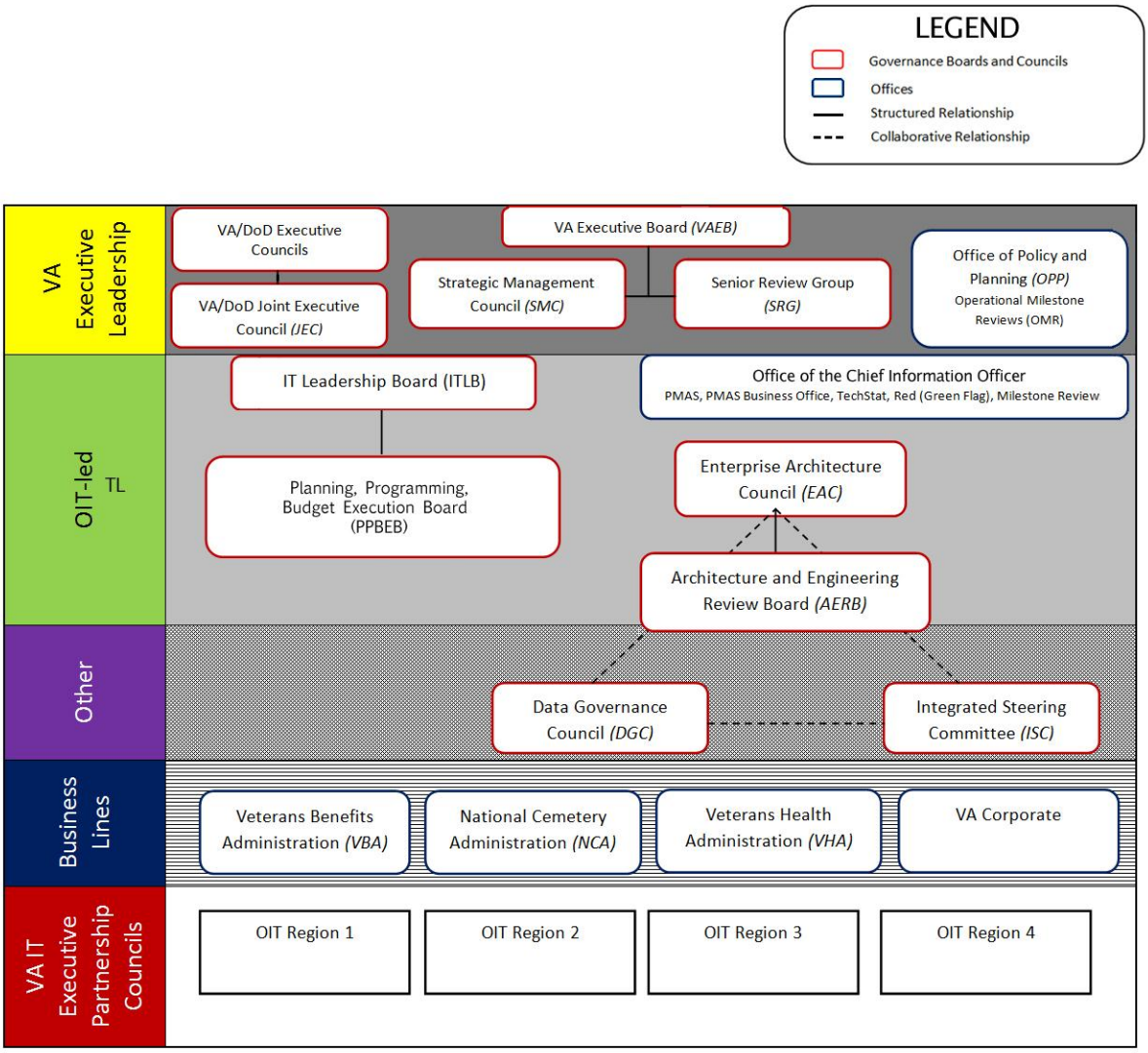

Figure 1. VA IT Governance Relational Structure

Figure 1. VA Governance Structure

5. ESTABLISHED ROLES AND RESPONSIBILITIES

Table 1. VA IT Governance Roles and Responsibilities

Body	Roles and Responsibilities	Chair	Interface/Relationships
IT Leadership Board (ITLB)	• Sets Department-wide information, security, and technology direction based upon business requirements and technology evolution. • Represents the information and technology services, strategies, principles, governance, and resources for all IT that supports business organizations across VA. • Approves and enforces IT policies.	Assistant Secretary for Information and Technology (AS/IT)	Provides IT counsel and recommendations to the Strategic Management Council (SMC) and VA Executive Board (VAEB). Adjudicates unresolved IT resource issues elevated by the BNTIB and PLTIB.
Planning, Programming, Budget Execution Board (PPBEB)	• Activities support collaboration and strengthen relations between the Office of Information and Technology (OIT) and VA Administrations and Corporate Staff Offices. • Confirms business needs and requirements, oversees risk, reviews funding requests and investments, reviews and recommends IT budgets in the near term and monitors IT program funding and financial execution. • Facilitate realization of business goals and supports and promotes improved efficiency, IT platform standardization, and stronger information security. • Ensures that VA IT business requirements are coordinated between business lines in the most effective and efficient way to support programs that enhance service to our Nation's Veterans. • Coordinates the development of the IT Multi-Year Program. • Ensures participant organizations' responsiveness and accountability throughout the programming process for IT investments. • Monitors alignment of IT programs and systems for consistency with the VA Strategic Plan, Enterprise Architecture, and VA IT Strategic Plan.	Deputy Assistant Secretary (DAS) for IT Resource Management (ITRM)	Facilitates near – and long-term issue resolution and appropriate coordination with the PPBEB to foster a synchronized IT governance effort. As appropriate, provides recommendations to ITLB for decision making.
Enterprise Architecture Council (EAC)	• Serves as the principal oversight body for VA's enterprise architecture, its implementation, and its governance. • Ensures coordination of architecture efforts, standards, and initiatives across the VA Administrations, business units, and Corporate Staff Offices. • Provides counsel and recommendations to the CIO and VA executive leadership regarding the enterprise architecture.	VA Chief Architect	Serves as a key vehicle for collaborative participation across VA. As appropriate, provides perspective and recommendations to the PLTIB, BNTIB, and ITLB. Coordination link with DGC and ISC. View EAC
Architecture and Engineering Review Board (AERB)	• Facilitates and guides the development, validation, publication, and maintenance of necessary enterprise architecture policies, standards, procedures and artifacts that are	Co-Chaired: Director, Enterprise Architecture	Reports to the EAC. View AERB

Body	Roles and Responsibilities	Chair	Interface/Relationships
	compliant with the OneVA EA. • Provides oversight, governance, coordination and a comprehensive control process that minimizes conflicts and duplication of efforts. • Ensures consistency between sub-architectures/solution architectures related to Major Initiatives, Core Mission Segments, and Service Segments. • Ensures IT projects are aligned with the OneVA EA. • Serves as the bridge between business/functional planning and IT strategy. • Encourages and maintains collaboration between the functional and technical communities to establish processes and tools to achieve its goals and deliverables.	And Deputy Executive Director, Enterprise Systems Engineering	
Data Governance Council (DGC)	• Serves as the principal entity which acts on behalf of the Secretary with respect to VA corporate data governance. • Acts as the final authority on all VA directives, policies, and standards involved in the creation, collection and dissemination of authoritative data. • Provides common processes and policies for collection, storage, retrieval, and dissemination of VA data. • Guides the enforcement of VA data standards for every IT project and business process initiative. • Designates and manages authoritative sources of master data.	Deputy Assistant Secretary, Data Governance and Analysis	Coordination and collaboration with VA Administrations and Corporate Staff Offices. Escalates issues not gaining consensus to the SMC for adjudication. View DGC
Integration Steering Committee (ISC)	• Supports integration opportunities across the major initiatives within the VA. • Establishes governance and processes to select and manage integrated veteran-facing capability delivery across the enterprise with the goal of improving service to Veterans and reducing redundant efforts.	Co-Chaired: Executive Director, Enterprise Program Management Office And VA Chief Architect	Coordination and collaboration with VA Administrations and Corporate Staff Offices. View ISC

6. CONSIDERATIONS

VA IT Governance has a component of ongoing maturity as appropriate to continue to institutionalize approaches to optimize governance to meet the business needs and provide IT solutions, services, and capabilities to meet the Department's mission in providing health care, benefits, and services to Veterans and their families which they have earned through their sacrifice and service to our Nation. With respect to the five capabilities/services listed below, as they mature from an information technology lifecycle perspective, they will be embedded in the VA's

Enterprise Architecture Compliance Criteria. As the Enterprise Architecture evolves, this will ultimately lead to better usage of the below five capabilities/services. The Department of Veterans Affairs Enterprise Architecture will be driver behind the enterprise-wide adoption of these capabilities/services.

7. POLICIES

7.1 Content Life Cycle Management

VA Directive 6102 addresses VA content life cycle management policies, and responsibilities for the planning, design, maintenance, support, and other functions related to the creation and administration of a VA Internet site, VA Intranet site, sites operating on VA's behalf and non-VA entities contracted to operate for VA. The Directive defines the organizational responsibilities for all web activities that govern and/or are related to posting, editing, maintaining, and removing files to or from the Internet and Intranet, the use of emerging Web-based technologies and new uses of existing approved technologies. The Directive emphasizes the importance of privacy-related issues, security requirements, accessibility requirements, the utilization of web applications and tools for enhanced performance and oversight, and the establishment of the VA Chief Information Officer's (CIO's) Office of Enterprise Development (OED), Resource Management Information Technology Development [RMIT 005Q]), as the entity which will have enforcement authority over all VA web activities. Directive 6102 is currently being updated. When the update is completed, revisions will be incorporated in this Information Technology Governance document.

VA promotes the secure and effective use of Internet services to improve access to and delivery of information to Veterans, their families, and the general public. VA also promotes the secure and effective use of Intranet services to improve access to and delivery of information to VA employees. Disseminated information will include the policies, programs, activities, and objectives of VA. Internet services will also be used to obtain information from public and private organizations consistent with applicable legal requirements. Internet and Intranet services will be used as a means of empowering employees in their work.

Organizational use of Internet and Intranet services must reflect the mission of VA, and support VA's goals and objectives. These services must support legitimate, mission-related activities of the VA and be consistent with prudent operational, security, and privacy considerations. Organizational use of government office information technology (IT) (equipment, peripherals, etc.) should be consistent with the provisions of any applicable VA Directive.

VA Internet and Intranet sites and sites operating on behalf of VA must be designed to support the widest range of potential users and computing platforms and must be compliant with Section 508 of the Rehabilitation Act.

7.2 Use of Web-Based Collaboration Technologies

VA Directive 6515 provides mandatory instruction for all VA offices and employees regarding the use of emerging Web-based resources and tools to facilitate collaboration, outreach,

communication, and information sharing at VA. These web-based collaborative tools include social media such as wikis, blogs, mashups, folksonomies, Web feeds (such as Really Simple Syndication [RSS] feeds), and forums (such as Facebook and chatrooms) and collaborative tools such as Microsoft SharePoint. Directive 6515 addresses general use policies, as well as policies relating to privacy, security, and accessibility. VA personnel and organizations using these technologies are responsible for ensuring that their use complies with applicable laws, regulations, and policies, including guidance from the Office of Management and Budget, and VA Directives and Handbooks 6102, Internet and Intranet Services and 6500, Information Security Program. VA offices and officers responsible for the governance of web-based collaboration technologies are outlined in Directive 6515, which provides descriptions of their specific responsibilities.

7.3 Adoption of Third-Party Online Tools

VA has a number of documents that control the manner in which VA applications are built, the products that may be used, the manner in which they can be used, and how they are selected and made available within VA. These documents include the following:

- OIT Strategic IT Principles
- Enterprise Application Architecture
- Release Architecture
- Technical Reference Model

The OIT Strategic IT Principles require that all products that are used are in the Technical Reference Model (TRM) before they are incorporated into a VA solution. It is further required that all products be from mainstream vendors able to support the product across the VA, nationwide. The Enterprise Application Architecture (EAA) incorporates the Strategic IT Principles and requires that applications be built on a standard stack of products to be defined and developed by VA Product Development (PD) and ESD. The standard stack of products for each data center is specified by the Releases Architecture (RA). The EAA requires that developers use a supported product stack and build unique solutions. Therefore, developers will have to adhere to a much more restrictive set of products than allowed in the TRM.

The EAA specifies a layered architecture with formal interfaces between the layers which allow the substitution of products at any layer, including the replacement of products at any layer with Commercial Off-the-Shelf (COTS) products or even cloud-based products. Therefore, the EAA allows the use of such cloud products once they are incorporated into the standard stack and have been engineered by ESD, approved by VA security, and incorporated into the TRM. Their use is subject to any constraints inherent as part of their inclusion in the TRM.

7.3.1 Establish that Tools Are Used to Promote VA Mission

There are two instances in which such tools might be acquired and employed: (1) where they are to be used as part of the application infrastructure stack, and (2) where they are to be used as a “functional” COTS tool incorporated to meet specific business requirements and used by a single application. An example of the first instance is a product that promotes sharing among VA

personnel or communication between VA and Veterans, but does not itself provide any content. An example of the second instance is a product that provides access to a community of users (for example, physicians or stakeholders for discussions regarding certain types of drug reactions or best practices).

The EAA requires that developers design and develop applications based on one of a limited number of infrastructure stacks where each stack is (1) supported by the VA (e.g., by a data center); (2) has been engineered by Systems Design and Engineering (SD&E); (3) has been reviewed and approved by appropriate VA security and privacy organizations; (4) has passed or can pass the VA certification and accreditation (C&A) process; (5) has been incorporated into the VA Release Architecture; and (6) has been incorporated into the TRM. Each of these steps assures that the products that developers are allowed to use have been thoroughly reviewed and are needed to support VA applications, and that the solutions meet VA security and privacy requirements, e.g., restrictions related to the dissemination of personally identifiable information (PII) and personal health information (PHI) as well as other classes of protected information that VA processes and stores. While a specific organization or data center may support more than one such stack, no stack will include multiple products performing the same purpose. The review process will assure that the products in the stack are required to support the applications that run on that stack.

Functional COTS are application-specific products that are intended to support the business needs of a specific application and thus, will not have been included in any of the infrastructure COTS. Such products will need to have been incorporated into the TRM prior to their use by any VA project and, thus, will have been through the TRM processes to determine that the products are required by the business application and are not duplicated by other products in the TRM. The project that proposes use of the tool must justify the business need for the project as part of the TRM review process assuring that the product is not approved unless it can be shown to meet a business need.

7.3.2 Ensure Terms of Service Are Legally Acceptable

The TRM and RA describe the tools that may be used to build VA applications and that can be incorporated into VA infrastructure. They do not provide a mechanism to acquire or gain access to the tools. The tools may only be introduced into VA through an acquisition effort that is supported by the VA acquisition and acquisition review processes. Therefore, VA can be assured that products will only be introduced into the VA environment after they have been acquired through approved acquisition processes performed by the VA contracting staff. The VA acquisition process includes legal review of all contracts. Since all acquisitions are performed by VA contracting personnel, VA can be assured that the terms of service are legally acceptable and fully compliant with approved GSA processes. The VA Office of Acquisition Operations has oversight responsibility on behalf of the Secretary to ensure VA complies with laws, policies, and directions from executive branch partners, such as the Office of Management and Budget, Department of Treasury, General Services Administration, Government Accountability Office, and Congress.

7.3.3 Guard Against Association with Legally Problematic Companies

As noted above, all tools and products incorporated into the VA infrastructure or VA IT solutions must pass a number of technical and governance reviews as well as a series of acquisition processes, and security and privacy reviews. They also must be engineered into VA solutions and be reviewed as part of the life cycle management process of the systems/projects that implement them. These processes will provide assurances that the VA does not deal with and is not associated with “legally problematic” companies.

A large number of VA personnel and contractors are provided with VA owned IT equipment, such as desktop computers, laptop computers, Personal Digital Assistants (PDAs), smartphones, etc. VA and contractor personnel with VA provided equipment are prohibited from installing software – other than the VA provided and approved software – on VA provided IT equipment. Other personnel are allowed access to the VA network through personally owned equipment; however, such access may only be made through the VA VPN and is provided in an isolated operational environment that prohibits installation of unapproved applications. Therefore, third party applications which a user may install on personally owned equipment are blocked from interacting or interoperating with VA systems.

7.3.4 Protect Agency Content

Any agreement to allow VA content to be stored or processed outside of VA must include contractual assurances that VA content is not modified inappropriately or removed, much like the assurances required for any agency data that is processed and stored in Contractor Owned / Contractor Operated (COCO) data processing facilities. Were VA to avail itself of cloud services to merely perform the work of its own applications the situation would be analogous to the traditional COCO solutions in that VA would own the applications and the data. Contractually, the issue is obtaining the data.

In more modern situations, the problem may be much more complex. For example, in a Software as a Service (SaaS) solution, the contractor will own the application, and even if VA were to assert ownership of the data, the data might be of little use without the application. Even if the VA were to have its own instance of the software, there would need to be specific contractual language guaranteeing that the VA data be made available to VA in a useful form.

The situation is even more complicated in cases of VA personnel using web-based social applications, such as Twitter. In cases involving social media, there may be no body of “VA data” per se, as VA data may be mixed with that of other users. For web-based social applications, it is not clear that VA data can be protected by the service provider. Therefore, there must be very strong VA direction regarding the information that may be shared through social media, as well as rules governing those who are tasked to officially represent the VA on social networks.

7.3.5 Ensure System Availability

The VA EAA specifies that VA applications be designed based on one of three levels of overall system availability. Overall system availability includes both scheduled and unscheduled downtime. The three levels are:

- Mission critical (99.999% available) or 5.3 minutes per year,
- Mission important (99% available) or 87.6 hours per year, and
- Generally important (95% available) or 438 hours per year.

As part of the application design and review processes, projects must specify:

- Which level of availability the system will be required to meet,
- The business basis for the selection of the level of availability, and
- Technical and management aspects of the project that assure the system will provide the specified level of availability.

Further, any project that uses an outside vendor to support the application processing will be required to:

- Have acquired access to the solution provider and assured that the terms of the service are sufficient to provide the required level of availability,
- Carry a risk that the outside vendor may not be able to meet the required availability and performance criteria and will need to have identified a risk mitigation strategy based on the sensitivity, criticality, and timeliness requirements of the data that are being stored or processed externally.

7.3.6 Provide Guidance on Use of Open Source Software

VA strongly supports the incorporation of open source software into its solutions. This effort is two-fold. First, encouraging the use of open source software into VA solutions; and, second, the far more novel approach of making internally developed solutions open source.

Wikipedia describes the Veterans Health Information Systems and Technology Architecture (VistA) as:

> *"… an enterprise-wide information system built around an Electronic Health Record (EHR), used throughout the United States Department of Veterans Affairs (VA) medical system, known as the Veterans Health Administration (VHA) It consists of nearly 160 integrated software modules for clinical care, financial functions, and infrastructure.*
>
> *The VHA manages the largest medical system in the United States providing care to over 8 million veterans, employing 180,000 medical personnel and operating 163 hospitals, over 800 clinics, and 135 nursing homes throughout the continental U.S., Alaska, and Hawaii on a single electronic healthcare*

information network. Nearly 25% of the nation's population is potentially eligible for VA benefits and services because they are Veterans, family members, or survivors of Veterans.

Over 60% of all physicians trained in the U.S. rotate through the VHA on clinical electives, making VistA the most familiar and widely used EHR in the U.S. Nearly half of all U.S. hospitals that have a complete (inpatient/outpatient) enterprise-wide implementation of an EHR are VA hospitals using VistA."

The VA has made VistA source code available to medical centers throughout the United States. VA recently donated the VistA source code to Open Source Electronic Health Record Agent (OSEHRA). Now VistA, the core system used by the Veterans Health Administration (VHA), the largest IT user within VA, is entirely open source. VHA accepts new releases of VistA from OSEHRA and submits proposed changes to OSEHRA. New releases of VistA will be based on OSEHRA releases. Therefore, VA's largest application is now and in the future will be an open source product supported by a nationwide community of VA and non-VA users.

In addition to making its largest application open source, VA also supports the use of open source products in its infrastructure tacks and product designs. VA IT Architecture Principles specify that the solutions with the lowest total life cycle cost – including acquisition and support costs –support the use of open source software. The stipulation is that there must be an organization available to provide support for the product across the enterprise. The preferred approach within VA is that taken with Red Hat Enterprise Linux (RHEL), in which a commercial organization provides support for an open source product.

Open source software must go through the same selection and acquisition processes as commercial software, including inclusion in the TRM, being engineered into VA solutions, and passing VA security and privacy reviews. The lower cost of open source software should make it a viable competitor in any VA software selection. The OSEHRA community has provided open source solutions in response to VA software RFIs. VA welcomes open source solutions and is currently implementing open source infrastructure products such as an open source Enterprise Service Bus (ESB) and is investigating open source NoSQL DBMS.

7.4 Mobile Application Delivery

VA is moving forward with full integration of mobile technologies in the VA enterprise. As part of this mobile initiative, VA is reviewing its application development processes to streamline them, making them more agile while maintaining the integrity associated with the VA brand. The mobile atmosphere is one that drives fast development, quick updates, and a constantly evolving environment that requires the agency to move quickly along with it. The procedures VA is developing will take into account the fast pace of the environment, apply successful VA processes (PMAS), and make modifications to cut down on the time to delivery. This approach not only takes advantage of technology that can change the shape of VA's delivery of services, but it also takes into account the need for the strong integrity expected.

VA's approach is to utilize the platforms that can support VA's security, management, and user requirements, rather than supporting or endorsing a specific platform.

VA promotes the use of open source, commercial-off-the-shelf (COTS) applications over customized applications that require more resources (staff and money) to develop.

VA has purchased and begun implementing a Mobile Device Management (MDM) system to secure mobile devices and facilitate updates of mobile applications.

7.4.1 Native Application vs. Mobile Web Application

The decision whether to use native vs. mobile web applications should be driven by user requirements. Native applications are quick to develop and can serve a variety of use cases, but only if they can be protected properly. Mobile web provides a device-agnostic, risk-reduced, environment. There are pros and cons for both native and mobile web applications, and decisions regarding platforms will be based on user requirements. If there are native apps that meet user requirements, then VA will pursue those. If web applications meet the requirements, then VA will pursue those. Ultimately, VA will pursue solutions that can meet the requirements and push developers to find ways to have mobile applications use native functionality.

7.5 Shared Infrastructure and Digital Information

VA supports policies promoted in the Federal Information Technology Shared Services Strategy, part of the Office of Management and Budget (OMB) *25-Point Implementation Plan to Reform IT Management*. This strategy, commonly referred to as the "Share-First Strategy," seeks to increase return on investment, eliminate waste and duplication, and improve the effectiveness of IT solutions.

In October 2012, VA issued a Draft Directive establishing enterprise-level authority and processes for identification, definition, implementation, usage, and monitoring of Enterprise Shared Services (ESS) including Service Oriented Architecture (SOA)-based services. The Office of the Assistant Secretary for Information and Technology (OIT) is responsible for issuing this policy and ensuring adherence to the policy across OIT. Deputy CIO for Architecture, Strategy, and Design (ASD) will act as its agent in performing this responsibility.

The Directive outlined the following for Enterprise Shared Services:

- Establish a federated governance framework supporting the development and operations of enterprise shared services.
- Establish ESS/SOA architecture principles that include standards, guidelines, design methodology, and security consideration.
- Establish an architectural assessment process for development and use of shared services.
- Develop a plan to communicate enterprise policy for shared services to business and IT architects and project managers.
- Develop ESS/SOA core infrastructure capabilities in alignment with the iEHR architecture.

- Develop a cost model to sustain both development and operations of enterprise shared services.

Establishing ESS/SOA within the Department will help reduce the overall cost of development through reuse of common SOA Services. The ESS/SOA design principles, standards, and guidelines are key methodologies and tools to be used for design, development, and assessment of enterprise shared Services. Existing SOA Services will then be accessible as a service and other teams will be able to leverage that service's functionality and value instead of re-creating it. As a result, the time to access that functionality will be reduced. Finally, ESS/SOA is a better way to support the Veterans and their spouses, survivors, and dependents by eliminating the requirement to reenter customer information among disparate information systems.

The Draft Directive outlines specific policies for all systems producing or consuming services, including (a) a governance body for implementation of the ESS/SOA initiative, (b) a governance framework to identify and analyze core areas for improvement, establish plans for a proposed increment, define and implement a transition plan, and monitor effectiveness of the governance regimen, (c) strategy and architecture guidance including incremental improvement, cost-benefit analysis, commonality and reuse of services, and a focus on high areas of volatility and most essential services, (d) capabilities and tools required as part of the implementation with ESS/SOA, including Service Taxonomy and Catalog, Service Registry, Enterprise Service Bus, Enterprise Service Definition Framework, Enterprise Service Level Agreements, Enterprise Service Operations, Test and Evaluation Certification, Enterprise Service Usage and Performance compliance, and Enterprise Service Feedback.

Details on these policies and the roles and responsibilities for enterprise shared services will become part of this Information Technology governance document once the Directive is finalized.

7.6 Data Management and Inventory

In October 2012, VA recommended establishment of an OIT Enterprise Data Management Office (EDMO) to concentrate development activities associated with data management into a single office within VA *(VAIQ #7264214)*. Currently, data design, analysis and documentation are performed by various organizations, including Product Development (PD), SDE and ASD. The result has been inconsistent design approaches, duplicate tables and databases, and inconsistent hiring and training practices for data oriented staff. To remedy these inconsistencies and redundancies, it was recommended that OIT EDMO be established in the OIT Office of Product Development and that EDMO be responsible for the following data management activities:

A. Defining standards and best practices to guide project development teams developing the Data Implementation Architecture for each VA application development, modernization, or enhancement project.

B. Defining standards and patterns for designing and developing Data Access Services to ensure that the authoritative instances of data are updated in a timely manner.

C. Ensuring that data entered into Online Transaction Processing Systems (OLTP) are extracted and made available to Operational Data Stores (ODS), the Enterprise Data Warehouse (EDW), and Data Marts.

D. Ensuring that designed and implemented databases and data stores do not provide for business logic direct access of any information stored in the data layer except through a formal service or direct API.

E. Performing the day-to-day data management activities assigned to PD.

F. Ensuring that all VA application system design, development, and enhancement projects conform to VA data management principles, VA Enterprise Data Architecture and policies.
   a. Determining that data design will protect PII and PHI to ensure that there is no inadvertent disclosure and to be able to prevent and / or detect malicious disclosure; advising project managers on required and recommended remediation.
   b. Reviewing VA applications and application designs for conformance; advising project managers on required and recommended remediation.
   c. Reviewing all contractor developed application designs and delivered systems to ensure technical conformance; advising project managers on technical acceptability and documenting required and recommended remediation.

G. Defining standards and best practices for developing the following entities, and providing consultation to project development teams on:
   a. Data Models and Database Designs
   b. Data Access Services
   c. Data Transformations

H. Serving as the Technical Steward responsible for ensuring the accurate implementation of data management systems as specified by the requirements of the functional data steward, through oversight, standardization and guidance of databases and data stores and the systems and services used to access the data. Also responsible for ensuring implementations utilize enterprise-standard data definitions, avoid redundant data collection, use authoritative sources of data where possible and adhere to departmental data governance guidelines.

I. Submitting updates to ProPath to incorporate the requirements of this memo.

New roles and responsibilities for data management and inventory across OIT were outlined in detail in the recommendations and, once approved and established, will become part of this Information Technology Governance document.

7.6.1 Security, Confidentiality and Privacy of VA Data

VA has established policies and procedures to secure VA information systems and applications that store, process or transmit VA information by, or on behalf of VA. These security requirements are designed to protect VA data assets and the personal, private information of VA employees, Veterans, their families and stakeholders. VA policies and procedures follow federal guidelines, including National Institute of Standards (NIST) requirements; Federal Information Processing (FIPS) standards; and Electronic and Information Technology Accessibility Standards from Section 508 of the Rehabilitation Act. The VA's established policies and procedures are outlined in a variety of Handbooks, including those listed below.

Handbook 6500: Risk Management Framework for VA Information Systems - Tier 3: VA Information Security Program

This Handbook provides the risk-based process for selecting VA information technology system security controls and operational requirements to implement VA Directive 6500. The Handbook is based on National Institute of Standards and Technology Special Publication 800-53, Rev. 3,

Recommended Security Controls for Federal Information Systems and Organizations, system security controls.

Handbook 6500.1: Electronic Media Sanitization

This Handbook (a) establishes a consistent, standards-based policy for the sanitization of VA electronic media which stores or processes VA information by, or on behalf, of VA; (b) defines procedures to be implemented by VA staff to sanitize and document the sanitization of electronic media that store or process VA information by, or on behalf of, VA; and (c) describes the responsibilities of personnel involved in the sanitization process.

Handbook 6500.2: Management of Data Breaches Involving Sensitive Personal Information (SPI)

This Handbook establishes procedures for VA management of data breaches involving VA Sensitive Personal Information (SPI). It implements 38 U.S.C. §§ 5721-28; and the implementing regulations at 38 C.F.R. §§ 75.111-119, section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act (codified at 42 U.S.C. § 17932) and interim final regulations at 45 C.F.R. §§ 164.400-.414, and Office of Management and Budget (OMB) Memorandum M-07-16, *Safeguarding Against and Responding to Breach of Personally Identifiable Information*.

Handbook 6500.3: Certification and Accreditation of VA Information Systems

This Handbook establishes procedures to ensure compliance with Certification and Accreditation (C&A) requirements for VA information systems as required by the Federal Information Security Management Act of 2002 (FISMA); Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources*; and VA Directive and Handbook 6500, *Information Security Program.*

Handbook 6500.5: Incorporating Security and Privacy into the System Development Life Cycle

This Handbook establishes VA policy, responsibilities and processes for incorporating security and privacy in the system development life cycle of VA IT assets that store, process or transmit VA information by, or on behalf of VA.

Handbook 6500.6: Contract Security

This Handbook establishes VA's procedures, responsibilities, and processes for implementing security in appropriate contracts and acquisitions. This Handbook applies to all VA Administration and Staff Offices and pertains to VA sensitive information which is stored, generated, transmitted or exchanged by VA, a contractor, subcontractor or a third party, or on behalf of any of these entities regardless of format or whether it resides on a VA system or contractor or subcontractor's electronic information system(s) operating for or on the VA's behalf.

Handbook 6500.8: Information System Contingency Planning

This Handbook provides the specific procedures and operational requirements for implementing Information System (IS) contingency planning in accordance with VA Directive and Handbook 6500*, Information Security Program*, ensuring Department-wide compliance with the Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. §§ 3541-3549 and the security of VA information and information systems administered by or on behalf of VA. This handbook applies to all VA organizations, their employees, and contractors working for or on behalf of VA. This Handbook includes revisions based on the NIST SP 800-34 (Rev. 1) *Contingency Planning Guide for Federal Information Systems*.

Handbook 6502.1: Privacy Event Tracking
In accordance with provisions of VA Directive 6502, Privacy Program, and in order to centralize and monitor the complaint and privacy incident resolution process, VA has established a system for privacy event tracking. This handbook describes the responsibilities, requirements, and procedures for this process. The system for tracking privacy events, currently called the Privacy Violation Tracking System (PVTS), serves as a central repository of complaints and privacy incidents. The system for tracking privacy events provides a Department-wide log of complaints and privacy incidents that are registered by VA personnel, Veterans, or their dependents and beneficiaries under applicable Federal privacy laws and regulations. The complaints and privacy incidents are addressed by VA Privacy Officers (PO) in compliance with applicable Federal privacy laws and regulations.

Handbook 6502.3: Webpage Privacy Policy
This handbook provides procedures for implementing the privacy policy provisions of the E-Government Act of 2002, as well as relevant Office of Management and Budget (OMB) guidance relating to the posting of privacy policies on federal Web pages

Handbook 6502.4: Privacy Act Reviews
This Handbook updates department-wide procedures for Privacy Act reviews.

Handbook 6502.76507.1: Acceptable uses of the Social Security Number (SSN) and the VA SSN Review Board
This Handbook identifies acceptable uses of the social security number (SSN) and establishes the procedures to be followed to determine when a collection or use of the SSN is necessary.

Handbook 6508.1: Privacy Impact Assessment (PIA)
This document outlines Department-wide procedures for conducting Privacy Impact Assessments (PIA), and implements the policies pertaining to PIAs that are set forth in Department of Veterans Affairs (VA) Directive 6502, VA Enterprise Privacy Program.

8. REFERENCED DOCUMENTS

Secretary's 16 Transformation Initiatives

VA Directive 6102, Internet/Intranet Services

OIT Strategic IT Principles

Enterprise Application Architecture

Release Architecture

Technical Reference Model

Federal Information Technology Shared Services Strategy

OMB's *25-Point Implementation Plan to Reform IT Management*

October 2012 Draft Directive for Enterprise Shared Services (ESS)

VAIQ #7264214 OIT Enterprise Data Management Office (EDMO)

National Institute of Standards (NIST) requirements

Federal Information Processing (FIPS) standards

Electronic and Information Technology Accessibility Standards from Section 508 of the Rehabilitation Act

VA Directive 6515, Use of Web-Based Collaborative Technologies