

VA



U.S. Department
of Veterans Affairs

Information Resources Management Strategic Plan

Office of Information and Technology

DRAFT

May 15, 2013



Table of Contents

Executive Summary	1
Introduction	2
1 VA Strategic Objectives, Goals, and Priorities	3
1.1 Agency Priority Goals (AXXA).....	3
1.2 OIT Mission, Vision, and Strategic Priorities.....	4
1.3 Relationship between VA Strategic Planning and IT Strategic Planning (AXXB, CXXD).....	5
2 Chief Information Officer Roles, Responsibilities, and Organization (DXXA) 8	8
2.1 Office of Information and Technology	8
3 Governance and Management Processes.....	12
3.1 VA Executive Governance.....	12
3.1.1 VA Executive Board (VAEB) (CXXB, CXXD).....	12
3.1.2 Strategic Management Council (SMC)	12
3.1.3 Senior Review Group (SRG).....	12
3.2 IT Investment and Portfolio Management Leadership (CXXA).....	12
3.2.1 IT Leadership Board (ITLB)	13
3.2.2 Programming Long Term Issues Board (PLTIB)	13
3.2.3 Budgeting and Near Term Investment Board (BNTIB)	13
3.3 Portfolio Selection (CXXC, CXXD).....	14
3.3.1 Unfunded Requirements.....	15
3.4 IT Program Oversight.....	15
3.5 Project Management Accountability System (PMAS) (CXXE, CXXF).....	15
3.6 ProPath	16
4 Mission Capabilities – Creating a “Veteran-Centric” VA (GXXA)	18
4.1 Improving Services to Veterans (BXXA, BXXC).....	18
4.1.1 Digital Government Strategy.....	20
4.2 Secure Mobile Applications (BXXB)	21
4.3 Managing Information as an Asset (GXXA).....	22
4.3.1 Architecture	22
4.3.2 Customer Data Integration	22
4.3.3 Other Initiatives	23
5 IT Infrastructure Optimization	24
5.1 Maturing the IT Portfolio (HXXA).....	25
5.1.1 Strategic IT Sourcing Plan (CXXG).....	26
5.1.2 Enterprise Licensing (CXXG)	26
5.1.3 IT Infrastructure Portfolio Evolution (HXXB).....	26
5.2 Enterprise Shared Services (ESS) (HXXC)	29
5.2.1 Enterprise Shared Services Target State	30



6	Cyber Security, Privacy, and Business Continuity	31
6.1	Mission and Goals.....	31
6.2	Security and Privacy IT Investment Alignment (EXXA)	31
6.3	Security and Privacy Services.....	32
6.3.1	Continuous Readiness in Information Security	32
6.3.2	Continuous Monitoring	32
6.3.3	Securing Personal and Sensitive Information (GXXB)	34
6.4	Business Continuity (EXXB).....	35
7	Workforce Development and Accessibility	36
7.1	Competency Models and Diversity (FXXA, IXXA).....	36
7.1.1	OIT Workforce Strategic Alignment (FXXA)	37
7.2	Workforce Accessibility and 508 Requirements (IXXB, IXXC).....	38
	Appendix A VA 2013-2015 Enterprise Roadmap	39
	Acronyms.....	40
	Bibliography/References	43



Executive Summary

The Department of Veterans' Affairs (VA) is responsible for a timeless mission: To fulfill President Lincoln's promise –

“to care for him who shall have borne the battle, and for his widow, and his orphan”

Our vision is of a VA transformed into a high-performing 21st century organization – one that adapts to new realities, leverages new technologies, and serves a changing population of Veterans with renewed commitment. VA is building an institution around three guiding principles: we will be *people-centric, results-driven, and forward-looking*.¹

Transforming VA from a claims-centric environment to one centered on serving Veterans in a comprehensive pro-active manner presents tremendous challenges. First and foremost is changing the *culture* of VA. To service Veterans from a holistic perspective, we must think of ourselves as an enterprise providing a full range of integrated services and capabilities. With this change in thinking comes changes in the way we look at our policies, our business processes, and our approach to customer service and, ultimately, the information environment that serves and services the enterprise.

This VA Information Resources Management (IRM) Strategic Plan, and the accompanying VA Enterprise Roadmap, describes how VA IRM activities align to and support VA's transformation so that we can more efficiently and effectively accomplish our mission by anticipating the needs of Veterans and Service members. In conjunction with VA's overarching Strategic Plan, these documents present VA's enterprise-wide approach to VA's transformation.

This VA IRM Strategic Plan describes how VA governs IT investments and aligns IT and information resources allocated to VA to deliver a world-class, event-driven architecture that supports proactive administration of VA benefits. The Enterprise Roadmap provides greater detail to the transition plans of each of the Administrations and the IT organization. Together, these plans describe activities for utilizing IT resources to effectively and pro-actively meet the VA's mission to serve our Veterans and their families.

The VA IRM Strategic Plan and Enterprise Roadmap provide a comprehensive view of VA transformation in a consolidated format previously unavailable. By making this information available to the Veterans, our stakeholders, our partners and the public, it is our hope to improve the Department's ability to better serve our nation's Veterans.

¹ Veterans Affairs Strategic Plan Refresh FY 2011 - 2015



Introduction

About the Department of Veterans Affairs (VA)

With a workforce of approximately 294,000 employees, VA provides high-quality benefits and services to Veterans and their beneficiaries. VA healthcare facilities include 152 hospitals, 817 community-based outpatient clinics, and 300 Vet centers, providing a broad spectrum of medical, surgical, and rehabilitative care to approximately six million Veterans. VA also provides compensation and pension benefits to nearly four million Veterans and beneficiaries, supports 56 regional benefits processing offices, and constructs and maintains 222 national and state cemeteries as national shrines.²

The information technology (IT) capabilities and services to support this scale of service delivery to Veterans are significant. The VA Office of Information and Technology (OIT) is one of the largest consolidated IT organizations in the world. To meet VA's health and benefit delivery commitments, we rely upon a large and complex technology infrastructure. VA's IT technology profile consists of over 390,000 desktop computers, 37,000 laptops, 21,000 mobile devices, and 512,000 email accounts. The OIT workforce is made up of approximately 14,600 employees and contractors.³ Our annual information technology investment of \$3.3B is important to sustain the provision of benefits and services to Veterans and their beneficiaries.

About this Information Resources Management Strategic Plan

This IRM Strategic Plan (including the accompanying Enterprise Roadmap) documents how OIT's IRM activities help accomplish VA's mission and ensure that IRM decisions are integrated with organizational planning, budget, procurement, financial management, human resources management, and program decisions to provide continuous improvement in value. The VA's Chief Information Officer (CIO), supported by the Office of Architecture, Strategy, and Design (ASD), is responsible for the IRM Strategic Plan. Developing this IRM Strategic Plan is a collaborative effort among many offices across VA working together.

² VA CIO Annual 2012 Performance and Accountability Report FY12 (Draft), November 15, 2012

³ VA CIO Annual Report FY12 (Draft)



1 VA Strategic Objectives, Goals, and Priorities

VA's Strategic Plan Refresh FY 2011-2015 identifies three Integrated Objectives that the Administrations and staff offices across the Department support. In addition, VA has also identified three Agency Priority Goals (APGs) which represent the Secretary's highest priorities for short-term and high impact improvement in VA mission performance. The current VA Strategic Plan is under review and a new strategic plan will be released this summer. The impact to our IRM Strategic Plan will be assessed and the document will be revised accordingly.

VA's Integrated Objectives

1. *Make it easier for Veterans and their families to receive the right benefits, meeting their expectations for quality, timeliness and responsiveness*
2. *Educate and empower Veterans and their families through proactive outreach and effective advocacy*
3. *Build our internal capacity to serve Veterans, their families, our employees, and other stakeholders efficiently and effectively*

Reference: Department of Veterans Affairs VA Strategic Plan Refresh FY2011-2015

1.1 Agency Priority Goals (AXXA)

Each of the three APGs is focused upon improving direct service delivery to Veterans and eligible beneficiaries.

Eliminate Veteran Homelessness

Priority Goal Statement: House 24,400 additional homeless Veterans and reduce the number of homeless Veterans to 35,000. By September 30, 2013, working in conjunction with the Interagency Council on Homelessness (ICH), the Department of Housing and Urban Development (HUD), VA will assist homeless Veterans in obtaining employment, accessing VA services, and securing permanent supportive housing, with a long-range goal of eliminating homelessness among Veterans by 2015.

Eliminate the Disability Claims Backlog

Priority Goal Statement: Improve accuracy and reduce the amount of time it takes to process Veterans' disability benefit claims. By September 30, 2013, reduce the Veterans' disability claims backlog to 40 percent from 60.2 percent, while achieving 90 percent rating accuracy up from 83.8 percent, in pursuit of eliminating the Veterans' disability claims backlog (defined as claims pending more than 125 days) and improving rating accuracy to 98 percent by 2015.

Improve Veteran Access to VA Benefits and Services

Priority Goal Statement: Improve awareness of VA services and benefits by increasing the timeliness and relevance of on-line information available to Veterans, Service Members, and eligible beneficiaries. By September 30, 2013, increase the number of registered eBenefits users from 1.0 million to 2.5 million.

To achieve VA integrated objectives and the APGs, the supporting information environment is moving from disparate stovepiped processes and systems to a unified environment of integrated, interoperable business processes and technical services. Integration of VA's core processes and information is necessary to provide Veterans with high-quality and efficiently delivered benefits and services.



1.2 OIT Mission, Vision, and Strategic Priorities

OIT provides information technology support across the Department for the sole purpose of ensuring VA's mission, vision, strategic objectives, and APGs are met. In alignment with this purpose, OIT's mission is:

"We provide available, adaptable, secure, and cost effective information technology products and services to our VA customers, enabling VA staff to provide mission-critical support to our Nation's Veterans."⁴

OIT's vision is:

"To become a world class organization and industry leader in the delivery of IT products and services, information security, and innovation, and to provide VA staff with cutting edge tools needed to provide the best customer service possible to our Veterans."⁵

Technology and the resources required to support it underpin every aspect of the care, benefits, and services we deliver to Veterans. IT is no longer a siloed segment of the budget focused on computers and monitors. It is the vehicle by which VA is able to extend its reach through healthcare, improved benefits processing, and provision of enhanced customer care and service to Veterans and their beneficiaries.

To actualize the OIT mission and vision and plan the necessary activities, VA's CIO has developed five Strategic Priorities. These Priorities provide OIT leadership the necessary strategic guidance for decisions by anchoring all OIT activities to OIT's mission and vision and by providing general guidelines for prioritization of resources.

CIO's Strategic Priorities⁶

Customer Service is OIT's number one organizational priority and focuses on maintaining and improving OIT's relationships with its customers. Improving customer satisfaction is a multi-level, multi-faceted challenge. VA uses the American Satisfaction Customer Index (ASCI) methodology to track IT customer satisfaction in every facility, which allows us to compare results to those of similar organizations in government and industry. A number of additional efforts are underway to improve performance of various IT systems and processes, including the National Service Desk organization, the IT Service Improvement Council, the Information Security Officers (ISO) Customer Service Brochure, and the Occupational Safety and Health Administration (OSHA) national safety program.

⁴ VA IT Strategic Plan FY 2012 – -2015, November 2012

⁵ ibid

⁶ VA CIO Annual Report FY12 (Draft)



Next Generation Information Security embodies VA's commitment to meeting the highest standards in protecting sensitive Veteran and employee information. OIT is making advancements in information security through the following programs: the Visibility to Everything initiative (V2E), the Trusted Internet Connections initiative, the Citrix Access Gateway Implementation project, supporting Veterans Health Administration (VHA) in the VA Medical Device Protection Program, and the Continuous Readiness in Information Security Program (CRISP).

Product Delivery represents OIT's commitment to provide secure, reliable, and well-designed products on schedule for VA's Administrations and staff offices that ultimately ensure success of the APGs.

Transparent Operational Metrics are key to knowing how OIT is performing and where we need to improve. A variety of operational metrics have been implemented and are being used to drive management decision making, including the IT Performance Dashboard, Daily Incident Report, and Monthly Performance Report. This ability to measure key processes and adjust accordingly is central to our continuous operational improvement and allows us to improve the use of staff resources and make better investment decisions with taxpayer dollars. OIT is now revising the Monthly Performance Review to strengthen the linkage of metrics to VA strategic goals.

Fiscal Management is crucial to meet the rising demand for IT services despite budget constraints. OIT has met the rising demand for technology and achieved other benchmarks by taking full advantage of the 5% funding increase for VA from FY 2010 to FY 2013. Budget constraints are a continued reality for OIT and, in response; OIT has initiated the Ruthless Reduction Task Force, developed a Vendor Management Office, and deployed a Strategic Capital Investment Planning process and Automation Tool. All of these efforts are designed to create maximum efficiency and effectiveness in the use of the IT budget.

1.3 Relationship between VA Strategic Planning and IT Strategic Planning (AXXB, CXXD)

Close collaboration exists between the VA departmental strategic planning process and the planning and enterprise architecture (EA) team within OIT. This ensures alignment between VA objectives and OIT activities. The VA Office of Policy and Planning (OPP) leads the VA Strategic Planning Process, which involves examining changes in environmental conditions and understanding the long-term implications of current choices, developing alternate strategies for addressing the changing environment, and determining and validating the capabilities required to posture the Department for success in the future. The process results in the development of the VA Strategic Plan and establishes the Department's near-term strategic direction. As shown in Figure 1, the VA Strategic Plan is used as the foundation of the VA IT Strategic Planning Process.

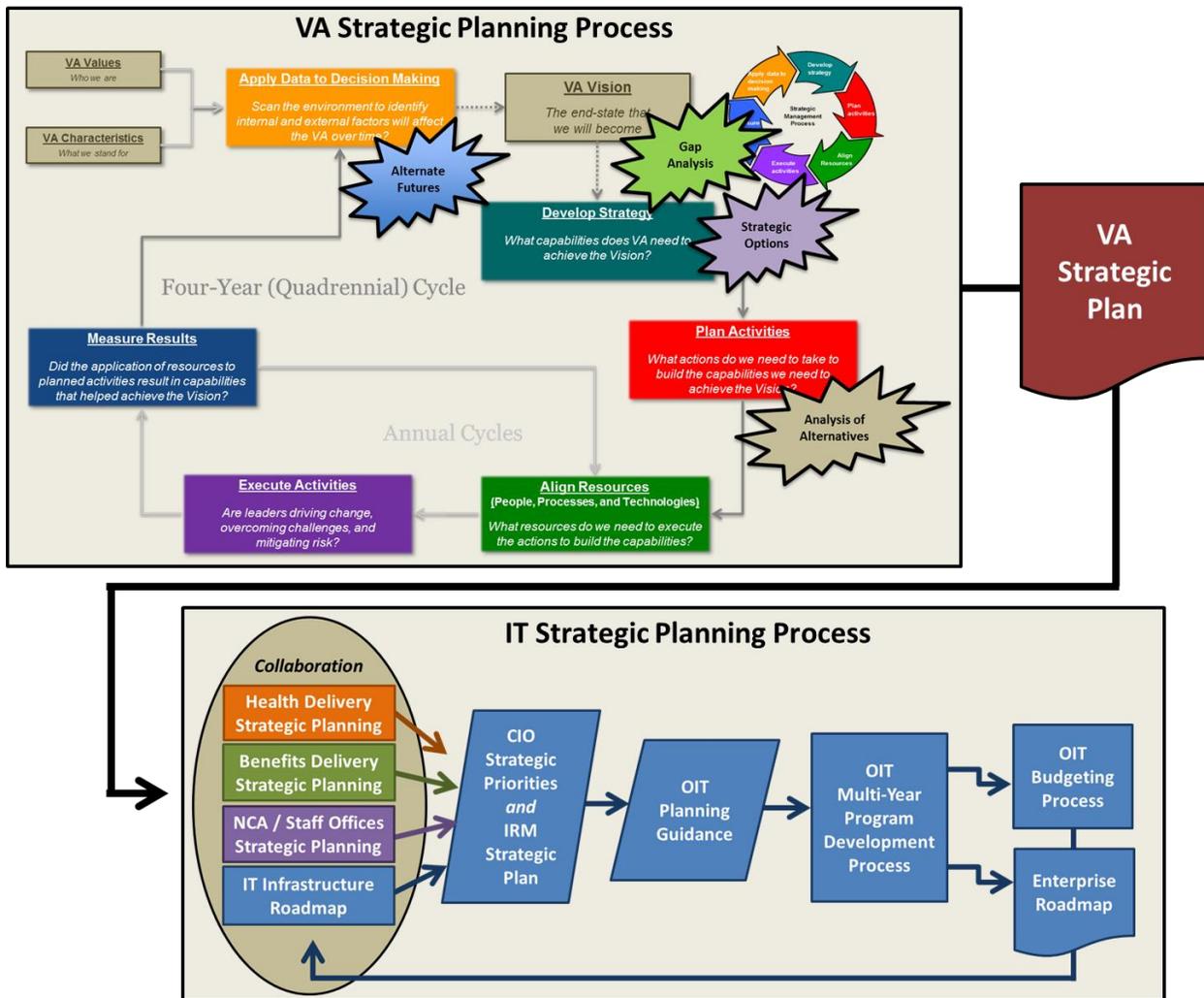


Figure 1: VA Strategic Planning Processes and Relationships

The VA Strategic Plan serves as the benchmark against which all VA Administrations and staff offices build their goals and objectives and plan investment activities, and it establishes a direct line-of-sight traceability from VA goals, objectives, and strategies to IT investments. As OIT supports all VA capabilities and services, the VA CIO and the OIT strategic planning team take into account the strategic plans from all VA stakeholders in developing the Department's IT vision, strategy, goals, and objectives. This includes using stakeholder input to inform the VA IT Infrastructure Roadmap, which lays out the future vision for VA network and infrastructure capabilities. OIT Planners weigh both business priorities expressed in individual VA Administration strategic plans and needs for VA IT infrastructure evolution, as expressed in the VA IT Infrastructure Roadmap, in developing the CIO's Strategic Priorities and this VA IRM Strategic Plan. These two artifacts initiate the internal IT strategic planning process pictured in the bottom half of Figure 1. The following presents those process steps in detail.



Collaboration – Customer Advocates leverage their relationships with senior leaders in the Administrations and staff offices to ensure that IT needs in support of mission capabilities are understood and reflected in OIT IT investment and development activities.

CIO Strategic Priorities – established to guide and inform IT investment and development activities through resource prioritization.

IRM Strategic Plan – describes VA’s IT resource management processes and activities and explains how CIO Authorities are executed within the Department. The IRM Strategic Plan describes how IT resource management activities support the accomplishment of VA’s missions and ensure that information resource management decisions are integrated with organizational Planning, Programming, Budgeting/Execution and Evaluation (PPBE), human resources management, and program decisions.

OIT Planning Guidance – The OIT multi-year strategic planning guidance published in March 2013 represents the first use of architecture and architectural constructs to inform the planning and programming efforts of the Department. This guidance provides the analytic framework for multi-year resource recommendations, ensuring that the requirements of VA’s healthcare delivery and benefits and memorial services are fully vetted and integrated in the FY 2015-2019 Multi-Year Program. This strategic planning framework guides the development of future year IT budgets to ensure alignment of IT capabilities and requirements with resources, thereby supporting the accomplishments of the Secretary’s strategic direction and the three APGs.

OIT Multi-Year Program Development Process (MYP) – This is a highly collaborative process that engages stakeholder from across the Department to establish priorities, construct alternative budget scenarios, and discuss resource needs for VA programs and projects over a five-year horizon. The outputs of the Multi-Year Program Development Process are numerous OIT Programming and Budget documents, as well as the Enterprise Roadmap.

OIT Budget Process – The two key artifacts developed during the OIT Budgeting Process are the Congressional Budget Justification, based upon the MYP, which covers a five-year planning horizon, and the Budget Operation Plan, which details the resource expenditure plan for the upcoming budget year.

VA Enterprise Roadmap – The VA Enterprise Roadmap provides insight into the state of VA’s transformation efforts. It describes the VA’s EA program and details for the Department’s most critical segments, current state and future visions of approaches, strategies, and initiatives in place to facilitate transition.



2 Chief Information Officer Roles, Responsibilities, and Organization (DXXA)

Within the CIO authorities as defined in statute and policy (e.g., U.S.C. § 38, 40 & 44 and Office of Management and Budget (OMB)-11-29) are assigned to and exercised by the Assistant Secretary for Information and Technology (AS/IT). The AS/IT serves as the principal advisor to the Secretary on all matters related to IT and Information Management. The AS/IT is specifically responsible for IT governance (including IT budget formation, IT strategy, and EA) and information security. The AS/IT is responsible for the optimization of VA's IT portfolio and for ensuring delivery of secure and robust services and capabilities across both VA's IT infrastructure and mission systems environments. The AS/IT is specifically charged with ensuring these environments are efficient, non-duplicated, and take best advantage of industry best practices such as commodity pricing and pervasive use of enterprise services. In addition to statutory CIO responsibilities, the AS/IT is also provided the authorities and responsibilities of managing the operations of VA's IT networks and leading all VA IT systems development activities through a single IT appropriation, and single IT authority – constituting the most empowered CIO in Federal government – with command and control authority over all IT staff, budget, contracts, space, and equipment.

2.1 Office of Information and Technology

The AS/IT exercises assigned authorities through OIT. Reinforcing VA's commitment to providing the very best services, OIT partners with VA's Administrations and staff offices, serving as a Veteran-centric provider of available, adaptable, secure, and cost-effective technology services, driven by five strategic priorities:

- Customer Service
- Next Generation Information Security
- Product Delivery
- Transparent Operational Metrics
- Fiscal Management

OIT activities include integrated business and IT planning; security and contingency planning to protect information and privacy across VA systems and networks; reviews to evaluate the performance of IT programs; review and approval of IT acquisitions; facilitation of intra- and inter-governmental partnerships; educating and informing the VA of IT-related, initiatives and legislation; and sharing lessons learned. To meet its responsibilities and challenges, OIT is organized as shown in Figure 2 below.

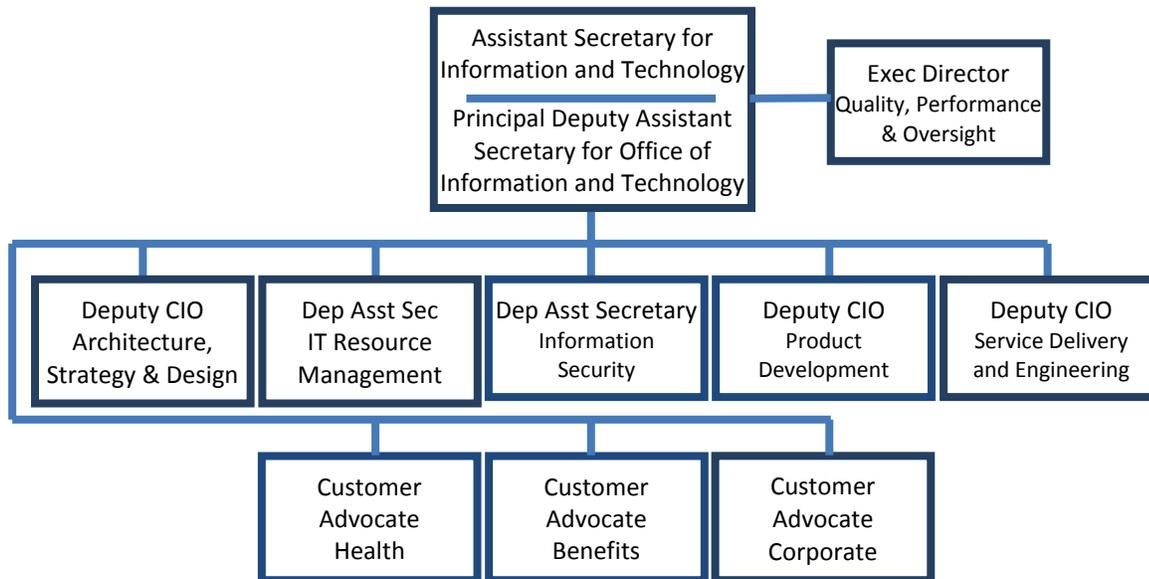


Figure 2: Office of Information and Technology (OIT) Organization Structure

Office of Architecture, Strategy, and Design (ASD) provides strategic planning and EA alignment and program development support for the VA IT environment, and defines the baseline, transition, and target capabilities necessary to optimize and maintain the IT environment. IT strategic planning results in the creation of VA’s IT vision, IT Infrastructure Roadmap, and IT investment guidance needed to support VA mission objectives. The VA Chief Architect establishes and manages the EA and IT strategy elements for VA as required in the Clinger-Cohen Act, in accordance with VA Directive 6051.⁷ ASD creates the IT strategy and leads the development of the multiyear planning guidance to drive strategic alignment of IT solutions and capabilities that serve Veterans’ needs while exercising proper stewardship of resources.

ASD is driving efforts to unify data architectures across VA to achieve data integrity, consistency, and availability across the enterprise in order to streamline development activities. ASD also supports stakeholders across VA in using EA to effectively guide and constrain strategic choices, investment decisions, and development activities.

Office of IT Resource Management (ITRM) is responsible for the management of all IT resources (including the IT budget), the direction of financial and IT asset management, and the policies and strategic planning activities for OIT acquisitions. ITRM links the budgeting process

⁷ VA Directive 6051 “VA Enterprise Architecture (EA),” July 12, 2002



with IT programs by directing the financial management, human capital management, IT asset management and procurement activities of OIT.

ITRM governs the VA IT portfolio, using the components of the OneVA EA, VA's enterprise architecture (EA), to link IT investments to mission objectives and business requirements. ITRM leads the IT investment review process and ensures that IT portfolio analysis is linked to annual budget development activities and aligned to strategic priorities.

Office of Information Security (OIS) ensures the security and privacy of Veterans' data. OIS ensures the confidentiality, integrity, and availability of information and information systems and works on matters related to information protection, including privacy, cyber security, risk management, records management, Freedom of Information Act (FOIA), incident response, critical infrastructure protection, and business continuity. The office develops, implements, and oversees the policies, procedures, training, communication, and operations related to improving how VA and its partners safeguard the personally identifiable information (PII) of Veterans and VA employees.

OIS conducts and integrates a continuous cycle of performance measurement, risk assessment, threat mitigation, oversight, and compliance to ensure that vigorous information security is in place, complements VA business operations, and is integrated throughout the life cycle of VA operating systems and software. OIS contributes to and supports the delivery of healthcare, benefits, and memorial services by validating process, system, and procedural compliance as well as ensuring that cost-effective security controls are in place to protect automated systems from fraud, waste, and abuse.

Office of Product Development (PD) delivers secure, reliable, and well-designed enterprise application software and services that serve Veterans and assist VA in achieving its goals. Day-to-day activities include planning, developing, acquiring, and testing applications that support the business sponsor and its requirements. PD comprises the following organizations: Project Management, Development Management, Product Support, PD Business Office, and the Program Management Accountability System (PMAS) Business Office.

PD has execution and oversight responsibility for all enterprise application development. Development consists of planning, developing (or acquiring), and testing applications that meet business requirements. PD provides IT program oversight (beyond CIO authorities) to centralize and oversee all program development. PD ensures visibility across all IT development activities to increase consolidation of application development, and promote the migration to services orientation, and support the standardization and reuse of services and applications.

Office of Service Delivery and Engineering (SDE) provides the infrastructure architecture, designs and implements infrastructure solutions, and directs all operational and maintenance activities associated with VA's IT environment. SDE oversees and manages the VA regional data centers and the IT network; monitors production for all information systems and production services, and delivers operations services (which include deployment, maintenance, monitoring, and support) to all VA geographic locations. SDE supports consolidated investment



planning, provisioning, performance measurement/management, and utilization of IT resources, aligned to the OneVA EA and IT strategic guidance.

SDE is responsible for IT logistics, campus management, administration, and resource planning across all IT operations. With a critical understanding of the needs and use of IT capabilities, SDE identifies opportunities to consolidate IT hardware, applications, services, and license agreements through Commodity IT investments.

OIT Customer Advocates (CAs) engage with VA Administrations and staff offices to ensure that IT issues of mutual concern are resolved. There are three CAs focused on healthcare delivery, benefits delivery, and corporate IT capabilities. CAs help ITRM and the Administrations to link achievement of agency mission objectives to IT investment and development activities. The CAs facilitate the resolution of questions related to the PMAS and work across VA to identify and facilitate the resolution of any IT issues relating to customer mission support. The advocates act as an Ombudsman between OIT and its customers, providing a single access point for customers to senior IT leadership.

Office of Quality, Performance, and Oversight (QPO) leads OIT's performance management, process improvement, and oversight efforts. QPO facilitates the establishment of performance measures and metrics related to the full range of IT program responsibilities and strategic objectives and manages associated measurement efforts. QPO also coordinates the Department's implementation of IT requirements for the E-Government Act of 2002 and is the primary contact for issues related to OMB E-Government.

Within QPO the Office of Enterprise Risk Management (ERM) is established to build a risk management capability that will provide an end to end solution in the management of OIT enterprise risk. The mission of ERM is to anticipate, identify, prioritize, manage, and monitor OIT enterprise risks and to provide assurance regarding the achievement of OIT objectives.



3 Governance and Management Processes

As discussed previously, VA has consolidated authority for all IT activities under the AS/IT/VA CIO. As such, the AS/IT engages senior leadership across VA in establishing Department-wide priorities and aligning IT activities with them. The AS/IT is responsible for both the formulation of the IT budget and management of the IT portfolio as well as the direct management control of all IT programs.

3.1 VA Executive Governance

The AS/IT CIO serves on all VA's senior executive boards, working with the Department's senior leaders to chart the overall course of the Department's capabilities. In this capacity the CIO has two main functions: providing an IT perspective on strategic and operational discussion and representing the interests of the OIT as the head executive.

3.1.1 VA Executive Board (VAEB) (CXXB, CXXD)

The VAEB is the Department's most senior management decision-making forum. It reviews, discusses, and, through the decisions of the Secretary, provides direction on Departmental policy, strategic direction, resource allocation, and performance in key areas. The VAEB is chaired by the Secretary and includes VA's Deputy Secretary, Chief of Staff, Under Secretaries for Health, Benefits, and Memorial Affairs, Assistant Secretaries, General Counsel, and the Chair of the Board of Veterans' Appeals.

3.1.2 Strategic Management Council (SMC)

The SMC serves as a collaborative and deliberative body that provides oversight and guidance on key strategic and operational issues that are likely to require action by VA decision makers. The SMC is chaired by the Deputy Secretary and includes VA's Chief of Staff, Assistant Secretaries, Deputy Under Secretaries for Health, Benefits, and Memorial Affairs, General Counsel, and Chair of the Board of Veterans' Appeals.

3.1.3 Senior Review Group (SRG)

The SRG serves as a collaborative and deliberative body that provides oversight and guidance on key strategic and operational issues and makes recommendations on issues that should be considered as part of VA's governance process. The SRG is chaired by the VA Chief of Staff and includes VA's Principal Deputy Assistant Secretaries, Chiefs of Staff for Health, Benefits, and Memorial Affairs, Deputy General Counsel, and Vice Chair for the Board of Veterans' Appeals.

3.2 IT Investment and Portfolio Management Leadership (CXXA)

The CIO reviews and approves the IT portfolio utilizing recommendations from the IT Investment governance boards, which provide the framework for decision making and accountability required to ensure that IT initiatives meet the strategic and business objectives



of the agency in an efficient and effective manner. The three boards, described below have been established to provide executive oversight to all of VA's IT initiative planning and management.

3.2.1 IT Leadership Board (ITLB)

The ITLB serves as the initial executive level review body for IT issues that impact VA business lines. The board adjudicates inter-board and intra-board issues of significance that cannot be resolved within the Programming Long Term Issues Board (PLTIB) and the Budgeting and Near Term Investment Board (BNTIB). In addition to approving the IT MYP, the ITLB makes recommendations regarding strategy, planning, budgeting, and execution of IT services to the SRG. The board also addresses budget formulation and execution issues that cannot be addressed by lower level boards. The ITLB is chaired by the AS/IT CIO and includes executive membership from each VA Administration and major staff office, including Under Secretary for Health, Under Secretary for Benefits, Under Secretary for Memorial Affairs, Assistant Secretary for Management, and Assistant Secretary for Human Resources and Administration.

3.2.2 Programming Long Term Issues Board (PLTIB)

The PLTIB serves as the initial management review body for IT issues that impact VA business lines. It focuses on long-term MYP planning and makes initial multi-year programming recommendations. The board establishes the IT appropriations annual budget for review by the ITLB and recommendation to the SRG. The PLTIB develops and updates a multi-year resources program that supports and adequately funds enterprise-level requirements through projects. The board functions in effect as a Portfolio Governance Board, reviewing the Departments' IT investment portfolio to identify wasteful, low-value, or duplicative systems through IT Portfolio review sessions. The PLTIB is chaired by the Deputy Assistant Secretary for ITRM/IT Chief Financial Officer (CFO). The members include senior executives from each VA Administration and major staff offices.

3.2.3 Budgeting and Near Term Investment Board (BNTIB)

The BNTIB confirms business needs and requirements, oversees risks, monitors budget execution at program and project levels, prioritizes unfunded requirements, and provides budgetary and financial reports. The BNTIB works collaboratively with the PLTIB to establish the IT appropriations current year Business Operating Plan (BOP). It focuses on execution of the annual IT BOP and recommends reprogramming actions during the fiscal year of execution. The BNTIB reviews the Department's IT investment portfolio to identify wasteful, low-value or duplicative systems through quarterly IT BOP review sessions. The BNTIB is chaired by the Deputy Assistant Secretary for ITRM/IT CFO and includes executive membership from each VA Administration and major staff offices.



3.3 Portfolio Selection (CXXC, CXXD)

Portfolio selection begins with the formulation of the MYP. The ITLB requests the CIO to issue a call and directions for the MYP formulation through the development and distribution of IT MYP Guidance for IT Investments. This guidance includes the governance and processes necessary to execute an efficient and effective MYP. It also includes target funding amounts and specific guidance for ongoing programs.

The Deputy Assistant Secretary for ITRM/IT CFO acts as facilitator for this process, issuing guidance and requests to VA's Administrations and staff offices to prepare descriptions of both ongoing programs requiring enhancements and new initiatives. The Deputy Assistant Secretary and the designated team hold multiple coordination sessions with stakeholders, including members of the PLTIB. The PLTIB establishes potential budget target scenarios based on current efforts and budget trends.

The PLTIB also approves criteria against which the initiatives will be evaluated. The criteria provide the means of prioritizing any proposed initiatives to ensure that the entire portfolio, once it is agreed upon, will meet the business strategy (as documented in the VA Strategic Plan). The criteria include identifying:

- **Project Benefit – Benefit to Veteran:**
 - **Veteran-facing:** Measures to what degree the project improves access and quality in the delivery of benefits and services to the Veteran.
 - **Organization-facing:** Measures to what degree the administrative or infrastructure project improves the enabling of the delivery of benefits and services within VA and ultimately to the Veteran.
- **Economic Impact:** Measures economic impact to VA, including change in sustainment or infrastructure costs; VA is assessing approaches to estimate return on investment (ROI), and use ROI in the prioritization process. In addition, is assessing approaches to include legacy system retirement as new systems are planned. .
- **Project Risk**
 - **Consequence of Inaction:** Measures the effect of projects in avoiding negative consequences, penalties, or mission degradation, or harm to reliability or stability of the operational environment.
 - **Maturity:** Measures requirements status and maturity of project to proceed.⁸

VA uses an automated decision tool to apply these criteria to proposed investments. The results form the foundation of the IT Portfolio. Projects are prioritized according to the

⁸ VA PortfolioStat 2012 Overview, Government Accountability Office (GAO) briefing, April 11, 2013



previously developed budget target scenarios and are then presented to the PLTIB for review and discussion. The PLTIB recommends the target scenario and plan that best represents the needs of the Department. The resulting IT Portfolio and MYP are then presented to the ITLB for approval and recommendation to the VA Executive Boards – principally the SRG.

The boards approve metrics that can be used in evaluating what each initiative will contribute to the overall implementation of the business strategy. The metrics will help the board to review the initiative objectives. When the portfolio is reviewed at a later date, the metrics can be used to determine if it was a success. Upon completion of the prioritization activities, the boards will make recommendations to the Department’s executives.

3.3.1 Unfunded Requirements

Unfunded requirements (UFRs) requests have become a normal component of business due to the budget-constrained environment of the OIT. The UFRs are submitted to either the PLTIB or the BNTIB depending upon the resource timing need. As of spring 2012, the Process Methodology Task Force (PMTF) was formed to add structure to the way UFRs are prioritized and funded. The PMTF is responsible for creating the prioritization criteria and data call templates and for outlining the criteria for the UFR voting. This new process engages OIT customers and ensures that spending is aligned to the Department’s Secretary and VA priorities.

3.4 IT Program Oversight

All IT system development within VA is done under OIT management. To ensure that development activities deliver expected capabilities within planned time and budget constraints, the - CIO has implemented the Project Management Accountability System (PMAS). PMAS stakeholders from across the Department are engaged in periodic formalized reviews of program status throughout the development lifecycle. These reviews monitor development progress, ensure alignment of activities with EA rules and standards, and provide an opportunity to review issues of interoperability with related programs within the IT portfolio.

3.5 Project Management Accountability System (PMAS) (CXXE, CXXF)

VA employs PMAS to manage projects with the VA IT Portfolio. PMAS has been implemented to ensure on-time delivery of IT capabilities. It establishes the governance framework and methodology to confirm that the customer, IT project team, vendors, and all stakeholders are focused on a single compelling mission – achieving on-time project delivery. Projects managed in accordance with PMAS are tightly monitored from start to finish and are subject to review by senior leaders when performance deviates from plan.

The PMAS process, from project authorization to project closure, begins when a project is included in the BOP and has been certified to Congress through the CIO Congressional Certification Letter. PMAS ensures both the readiness and the performance of an IT project



throughout its lifecycle, while ensuring accountability is met. The PMAS life cycle includes a progression of activities (called PMAS states) designed to develop and deliver capabilities, each subsequent one of which is entered only with the successful completion of the previous states' activities and confirmed at Milestone Reviews. The life cycle begins with the New Start State and extends through the successful completion of the Milestone 4 Review. PMAS States are defined as New Start, Planning, Active (generally divided into Active Development and Active Implementation states), and Closed.

The frequency of each project's Milestone review is defined by the project's planned duration in the PMAS states. For example, the frequency of Milestone 1 and 2 Reviews is dependent on the planned length of the increments, which can be no longer than six months. Each Milestone Review requires the completion of a defined set of project activities and artifacts. (See Appendix 1 – PMAS Milestone [MS] Review Requirements/Artifacts.)

Milestone Reviews function, in effect, as an Investment Review Board. They are chaired by the DAS/DCIO or his/her SES representative from the appropriate OIT office, and are convened weekly, at a minimum. A full spectrum of senior IT leadership, including the Principal Deputy Assistant Secretary for IT, the OIT Executive Leadership Team (comprising Deputy CIOs and Deputy Assistant Secretaries), and all applicable Offices of Responsibility within OIT are present at each Milestone Review and are actively engaged in approving a project's entry to the next level of IT development or deployment.

3.6 Enterprise Risk Management

Enterprise Risk Management (ERM) acts as an independent enterprise risk appraisal function by determining if OIT Enterprise risk management, controls, and governance processes, as designed and represented by OIT management, are adequate and functioning as anticipated. Risk owners manage and mitigate risk within their individual lanes of responsibility. The OIT ERM Office of Risk Management Planning (RMP) works with each OIT organization to identify and address risks that affect the enterprise as a whole. Once enterprise-level risks are identified and the impact to OIT business processes determined they are presented to the AS/IT. This enables the AS/IT and OIT executive leadership to make informed decisions on operations designed to provide services to Veterans and their families; and provides OIT the services it needs to achieve its mission. OIT ERM Risk Assessment and Mitigation (RAM) teams are available to assist the AS/IT and each OIT organization by performing root cause analysis assessments, recommending risk response and mitigation strategies, and performing post-mitigation assessments.



3.7 ProPath

ProPath is the companion to the Project Management Accountability System (PMAS). ProPath is an innovative, front-end tool to a Process Asset Library containing information regarding standard processes. It is a one-stop shop providing critical links to the formal approved processes, artifacts, and templates to assist project teams in facilitating their daily work.

ProPath was established in order to enhance and encourage standard, repeatable processes that can be utilized easily across the organization and is the first step in a long-term investment toward improving our development processes. It is the central resource that builds upon the Program and Development managers' delivery of high-quality products. Through an 'at-a-glance' perspective of nearly every step in the software development process, ProPath offers insight into the steps required, in the form of process maps, to ensure that IT activities and resources are focused on optimizing specific outcomes, rather than assets.



4 Mission Capabilities – Creating a “Veteran-Centric” VA (GXXA)

Like many organizations in today’s information age, VA is in the midst of information-driven transformation. Historically, VA has optimized around individual benefit programs with individual sets of business processes, rules, and even data sets. As a result, VA information systems exist to meet specific objectives without always taking into consideration the critical need of information consistency when reaching across services and querying information from different systems. The result has been that information about any individual Veteran is fragmented and incomplete. This paradigm no longer works in today’s environment.

Veterans today, like any other cross-section of society, are fully taking advantage of emerging information capabilities. This impacts their expectations of service quality and service delivery. They expect to be able to interact with VA anytime, anywhere. They expect anyone with whom they interact at VA to know who they are and what services they receive (or are entitled to receive). They expect service to be quicker and more streamlined. They are dissatisfied when they have to continue to provide VA the same information about themselves multiple times. With this backdrop, VA clearly has to evaluate how it engages and services its Veterans and to adopt new strategies for customer care.

VA has been embracing this challenge and adopting a “Veteran-centric” approach to deliver healthcare and economic benefits to Veterans through business processes that start with the needs of the Veteran – not the convenience of the VA. This involves establishing a relationship with every Veteran that starts the day they enter military service and evolves throughout their lifetime. To be truly “Veteran-centric”, VA’s goal is to not only provide the fastest and best service to the Veterans, but also to be proactive in doing it – determining wherever possible, ahead of need, Veterans’ potential health and financial benefits requirements and eligibility, and informing Veterans instead of waiting for them to come forward and ask.

4.1 Improving Services to Veterans (BXXA, BXXC)

VA has undertaken several major initiatives (both internal and Veteran-facing) designed to improve its delivery of services and benefits to veterans. These initiatives are also designed to help VA meet its APGs. Table 1 shows the how the Veteran-facing services are aligned to the APGs.

Agency Priority Goals	Veteran-Facing Services
Eliminate Veteran Homelessness (EVH)	EVH
Eliminate the Disability Claims Backlog	Veterans Benefits Management System (VBMS), Integrated Electronic Health Record (iEHR)
Improve Veteran Access to VA Benefits and Services	Veterans Relationship Management (VRM) eBenefits, My HealtheVet, Blue Button, Digital Strategy

Table 31: Service Alignment to APGs



Three of these services are highlighted below.

My HealtheVet:

My HealtheVet is a web-based application that creates a new, online environment where Veterans, family, and clinicians may come together to optimize Veterans' healthcare. Web technology will combine essential health record information enhanced by online health resources to enable and encourage patient/clinician collaboration. The implications of My HealtheVet are far-reaching. Clinicians will be able to communicate and collaborate with Veterans much more easily. The new online environment will map closely to existing clinical business practices, while extending the way care is delivered and managed. As Veterans build up their lifelong personal health records, they will be able to choose to share all or part of the information in their account with all their healthcare providers, inside and outside the VA. This has the potential to dramatically improve the quality of care available to our nation's Veterans. Through Veteran empowerment, each Veteran can better understand and manage their own health and better assess the potential gain and risk of proposed medical interventions. Key portions of the Department of Defense (DoD) Military Service Information are now available in My HealtheVet. This new feature is available to military retirees and/or Veterans discharged after 1979.

Blue Button:

The VA's Blue Button available for use on My HealtheVet enables Veterans to download, view, store and print information from their VA Personal Health Record. VA Blue Button feature offers My HealtheVet registrants the ability to download information currently in their My HealtheVet account. This functionality benefits Veterans by improving the quality and accessibility of their health information.

By using Blue Button, Veterans can print, save, or transfer My HealtheVet personal health information as a PDF, text file, and Blue Button output file. My HealtheVet Account History Activity log lets users track when Blue Button was used to download their health information. The goal is to get the data into the Veterans' hands and allow them to share personal health information with people they trust, such as family members, caregivers, or health care providers. Veterans who have been authenticated will have the ability to download and view VA Wellness Reminders, VA Appointments, and access various data from their VA electronic health record in My HealtheVet's VA Blue Button download. In December 2011, the VA launched a new feature of the Blue Button, which allows Veterans to download their Military Occupation Specialty (MOS) data.

In 2013, a new tool was added to the VA Blue Button: the VA Continuity of Care Document (VA CCD). The VA CCD is a feature that contains a summary of the Veteran's essential health and medical care information in an xml and pdf file format. The VA CCD uses recognized standards that support the exchange of information between health care systems and providers for effective continued care of the patient.



eBenefits:

The President's Commission on Care for America's Returning Wounded Warriors (Dole/Shalala) was established by Executive Order 13426 in March 2007. The Commission recommended the creation of a "My eBenefits" (aka eBenefits) web portal that would provide Service members, Veterans, their families and authorized caregivers with a single sign-on, central access point to clinical and benefit data.

eBenefits is a portal; a central location for Veterans, Service Members, and their families to research, find, access, and, in time, manage their benefits and personal information. eBenefits offers:

- A personalized workspace called My Dashboard that provides quick access to eBenefits tools. Using eBenefits tools, users can complete various tasks. The users can apply for benefits, download a DD 214, and view their benefits status, in addition to other actions as needed. This workspace is available to users once they have created an eBenefits account.
- A catalog of links to other sites that provide information about military and Veteran benefits.

The VA and DoD are committed to improving the online experience for Veterans and Service Members. Additional features and process enhancements can be expected in future quarterly releases.

Appendix A, the VA Enterprise Roadmap, FY2013-2015 provides more information on the full range of VA initiatives.

4.1.1 Digital Government Strategy

In its planning for Veteran-centric services, VA is taking advantage of the Federal Digital Government Strategy (FDGS), which was released May 23, 2012. The FDGS provides guidelines for all federal agencies for using modern tools and technology to build a 21st century platform to better serve the American People. VA is implementing the FDGS Milestones to deliver better digital services to Veterans, their families, and stakeholders as well as the VA workforce.

The FDGS stresses a "Customer-Centric" approach. This allows customers to help shape, share, and consume information whenever and however they want it. This approach influences how data are created, managed, and presented through websites, mobile applications, raw data sets, and other modes of delivery. VA is taking steps to ensure that digital services follow guidelines set forth by the Federal Digital Services Advisory Group and Federal Web Managers Council. Performance and customer satisfaction measurement tools have been implemented on va.gov websites. VA installed the General Services Administration (GSA)-provided Digital Analytics Program (DAP) tool, a custom version of Google Analytics Premier, which provides web performance metrics. The DAP tool provides customized dashboards to help VA track, compare, and analyze customer use of its websites and to inform decisions for improvements



to VA sites and service delivery. The tool has been implemented on all VA Tier I websites, with plans for phased expansion to Tier II and III websites, as those sites are updated with the agency's new user interface in VA's content management system.

Veterans and other users will have online access to services and benefits through a single portal that will then direct them to the appropriate application. VA uses the program *Foresee* to collect customer satisfaction metrics through online surveys. While the GSA provided DAP to agencies at no cost for use in gathering web performance metrics, there is not yet a government-wide tool for collecting and reporting the requested baseline customer satisfaction metrics.

VA is using social media to provide information to – and receive feedback from – Veterans and their beneficiaries. By implementing *Facebook* pages for every VA medical center, VA has reached 109,000 Veterans and their family members and dependents at a local level. The agency also uses *Twitter* to reach over 121,000 Veterans every day. VA uses *Flickr* and *YouTube* to provide photos and videos that highlight issues and events important to Veterans. *Flickr* and *YouTube* combined have been accessed 2.5 million times. The VA blog, *Vantage Point*, is also used to communicate key issues to Veterans.

In response to the FDGS directive to identify at least two existing priority customer-facing services to optimize for mobile use, VA performed data calls requesting information regarding planned, in-development, and provisioned mobile applications. Additionally, numerous face-to-face meetings and conference calls were held with various program managers and systems engineers across departments to validate what would later become the initial direct response to this milestone action. VA revised its initial data gathering approach and internally canvassed and prioritized its set of mission-essential mobile applications and provided a list of first-move candidates, including *Post Traumatic Stress Disorder (PTSD) Coach*, *Clinic in Hand Mobile Prescription Medication Refill*, and *Homelessness Mobile*. In May 2013, as required, VA will update the information on mobile application development plans, using the OMB MAX Collect Tool.

4.2 Secure Mobile Applications (BXXB)

VA is developing mobile applications to broaden its capacity to serve both internal and external customers – Veterans, their families and caregivers, and VA employees. The ultimate goal is to make healthcare, benefits, and employee tools digitally available from any location, at any time. Secure and private mobile access to services and information is based on a unique identifier used across VA IT systems, and properly understood by all external VA stakeholder entities that provide services to Veterans and Service members. VA has several mobile applications currently available. Two examples are the PTSD Coach, which provides Veterans and military Service members with information related to PTSD; and the Clinic in Hand Mobile Prescription Medication Refill, providing patients with the ability to refill medications using a mobile device.



VA mobile platforms are designed to the highest mobile security and privacy standards available. VA is actively monitoring discussions on mobile privacy and security and will incorporate new federal security requirements being developed by Department of Homeland Security (DHS), DoD, and the National Institute of Standards and Technology (NIST) for mobile and wireless services into its enterprise policies and procedures.

4.3 Managing Information as an Asset (GXXA)

Information and IT play a pivotal role in the transformation of VA into a “Veteran-centric” organization, wherein VA creates a single, integrated, and complete view of the Veteran. VA’s ability to provide benefits in a Veteran-centric manner rests on the ability to collect and manage information in such a way that it is secure yet discoverable, accessible, and understandable by authorized users anywhere, anytime. VA is building an information environment of interoperability and openness.

4.3.1 Architecture

VA began its enterprise architecture work in the summer of 2012 by holding a Data Summit, sponsored by the Chief Architect. The summit brought together stakeholders from across the Department, particularly from the VA Administrations involved in providing healthcare and economic benefits to Veterans. The participants agreed to work together to develop a Conceptual Data Model (CDM) of “common data” – data used by more than one Administration or staff office – to describe a Veteran. VA’s CDM for common Veteran data was published in the fall 2012. The CDM describes basic information about:

- Identity
- Military Service History
- Demographics
- Contact Information

VA is using this information to define and implement an Enterprise Logical Data Model (ELDM). The ELDM will provide a Department-wide view of data (and its attributes) used by Administrations and Staff offices at VA. This model will enhance and support data standardization, recognition of data redundancy, and potential institution of single authoritative data sources, physical data models, and synchronized, coherent system implementation.

4.3.2 Customer Data Integration

The Customer Data Integration (CDI) effort builds upon the work begun in 2012 by seeking to establish the foundation – policies, governance, processes, and services – required to manage



customer data as a Department asset.⁹ CDI will lay the groundwork for establishing data governance authorities within VA through a Corporate Data Governance Board, unified standards for data representation, and authoritative sources for common data. These standards will be implemented in every new IT project that has a requirement to use this data. The data governance authority will develop policies for the ways in which common information is collected, used, safeguarded, and archived or deleted.

Within the CDI initiative, leadership from across the Department's Administrations and staff offices have come together to first gain a clear picture of existing VA processes and data flows and then to address them in a systematic manner. The EA team is playing a lead role in this effort, using this commitment from the Administrations as the mechanism to leverage leadership across VA to build out the Department's existing process and data architecture. This represents a huge opportunity to engage every organization within VA in both the development and use of EA to help improve VA information management capabilities.

4.3.3 Other Initiatives

In addition to the CDI initiative, VA is pursuing other data-focused initiatives, including:

Virtual Lifetime Electronic Record (VLER):

VLER is an enterprise-wide VA initiative inclusive of partnerships with other federal, state, and private sector organizations. The purpose of VLER is to enable VA and its partners to proactively provide the full continuum of services and benefits to Veterans through Veteran-centric processes made possible by effective, efficient, and secure standards-based information sharing. VLER is a multi-faceted business and technology initiative that includes a portfolio of health, benefits, and personnel information sharing capabilities.

Identity and Access Management (IAM):

IAM enables VA to rapidly search, identify, and authenticate who is accessing its information systems. It is a critical aspect of meeting Department-wide and federal government information security mandates.

Integrated Electronic Health Record (iEHR):

iEHR is a joint effort with DoD to integrate electronic health records, enabling a full and seamless lifetime medical record for Veterans from accession to final care by providing a single, virtual, secure system of record for all medical information pertaining to active duty Service members, Veterans, and their beneficiaries.

⁹ Customer data represents the first instance of common data. Other classes of common data will be developed as the architecture is constructed.



5 IT Infrastructure Optimization

The VA enterprise IT infrastructure, which encompasses all corporate, mission-critical, and Veteran-facing IT systems, provides the backbone upon which OIT delivers the necessary technology and expertise to achieve VA’s mission, goals, and objectives. Figure 3 depicts OIT’s technology framework.

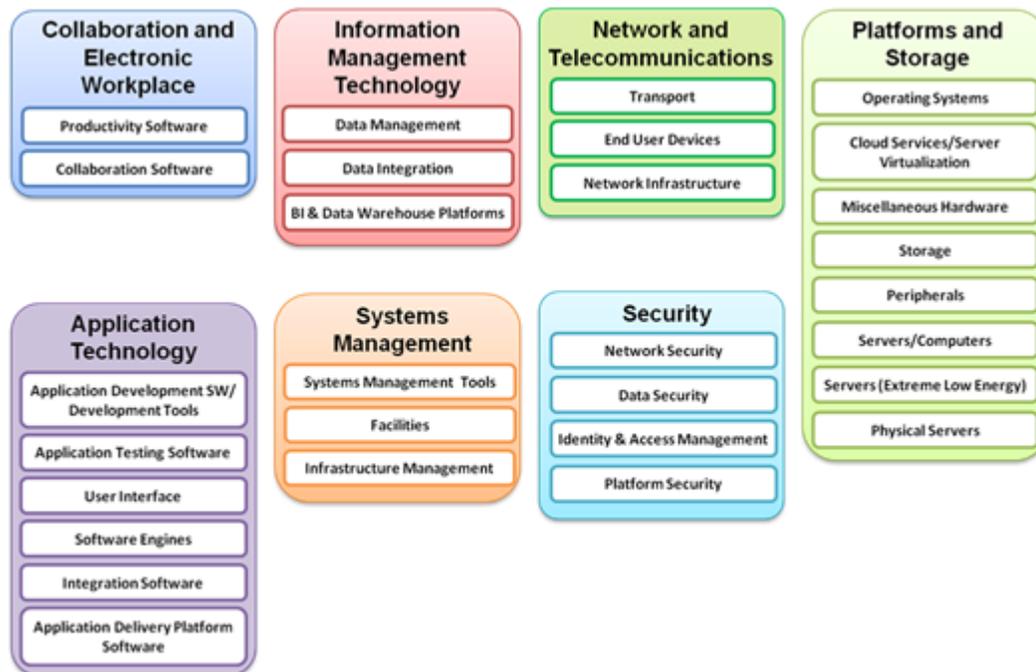


Figure 4: Technology Categories

OIT acts as a steward for all VA’s IT assets and resources. OIT employs enterprise systems engineering capabilities to establish and implement architecture and design rules, standards, and reference models for all IT system platforms and infrastructure, in accordance with the established VA EA, across the Department. VA maintains a highly available, scalable, and redundant infrastructure that substantially reduces the government’s risk and enables future IT service delivery growth.

VA’s IT infrastructure must be continually strengthened, optimized, and enhanced to enable continued and improved services to our Veterans, their beneficiaries, and the entire VA community. The efforts listed below were included in the OIT FY 2015-2019 Planning Guidance as part of the increased funding trade space area.

- Develop and execute a Unified Communication and Collaboration strategy that enables a converged platform serving all communications media (voice, data, video, chat, presence, and unified messaging).



- Transform VA networks into software defined networks in accordance with the IT Infrastructure Roadmap to enhance services, accommodate growing demand due to the increasing Veteran population, and enable emerging technologies such as mobile applications and cloud computing.
- Consolidate Data Centers to reduce redundancy and costs and to improve access to information.
- Implement the Enterprise Management Framework (EMF).
- Use reengineering with virtualization as the first strategy to meet server needs.
- Identify opportunities and implement plans for cost savings through careful management of enterprise licensing, optimizing unit cost versus focused provisioning of real need.
- Identify opportunities and implement plans for commodity IT investments.
- Support paperless administration of Veteran benefits.
- Support the increasingly mobile workforce.
- Support wireless infrastructure in facilities.
- Support migration to one central processing unit (CPU) device per user, that is, one device that communicates and one device that computes.
- Move to VA Cloud Computing where economically justified.

5.1 Maturing the IT Portfolio (HXXA)

OIT conducts a continuous effort to identify underperforming and/or inefficient IT investments and yield funds from those investments for reapplication toward high-priority efforts that require additional resources. Enterprise-wide initiatives such as the Ruthless Reduction Task Force (RRTF) focus on consolidating IT services, infrastructure, licenses, and business systems to drive costs down and optimize interoperability and accessibility.

VA is consolidating and optimizing its IT infrastructure through standardizing IT platforms and streamlining the deployment of systems across multiple business units onto those platforms. VA is increasing its use of commodity IT purchasing for hardware and software components, as well as enterprise licenses to consolidate and optimize investments and streamline maintenance and sustainment operations. Initiatives are underway to establish enterprise strategies for requirements identification and management, enterprise shared services, and mobile application development and deployment to reduce redundancies in developing mission capabilities and to capitalize on potential cost reductions emerging technologies. VA's future vision for the workplace includes using Network as a Service (NaaS) and shifting to a Commodity Cost Model (for devices and software) to benefit from economies of scale.



5.1.1 Strategic IT Sourcing Plan (CXXG)

The foundation of VA's IT sourcing plan includes situational analysis of the technology market aligned with OIT funding limitations and needs prioritization. The sourcing plan includes a depth and breadth of input from stakeholder groups as diverse as customer advocate organizations, administration customer service providers, program management officials, and Congress.

A long-time leader in healthcare IT, VA is expanding the strategic focus to the external marketplace as a supplier of information systems as a way to improve the quality of services provided to Veterans and their families. Innovations in the marketplace make it possible for VA to respond more effectively to a changing technological landscape to deliver timely and modern support to our nation's Veterans. In migrating toward a marketplace-based approach for provisioning VA information technology goods and services, the focus of how this is done has transformed to an enterprise level to achieve a higher level of consistency, uniformity, and quality across the organization. VA uses an annual strategic planning process that reaches down to the smallest field unit for input; needs are then prioritized, consolidated, and elevated to VA management officials responsible for enterprise operations. This type of strategic planning is intended to identify opportunities to acquire enterprise licenses for software, cloud services, hardware, and infrastructure in order to maximize value.

5.1.2 Enterprise Licensing (CXXG)

Enterprise licensing is an alternative to ad hoc licensing that is entered into predominantly when an economy of scale can be reached at a national level over regional, program, or locale-based purchase. Identifying opportunities for enterprise licensing begins with a view of VA's IT infrastructure and continues on into considerations for lifecycle replacement. The IT Logistics Office and Contracting activities work with IT leadership to coordinate the creation and sustainment of enterprise licensing. Unlike other aspects of IT product and service delivery, enterprise licensing receives a higher level of budget priority over individual purchases. When considering the next generation of software, OIT works with software vendors and the open source community to determine if software under consideration can be deployed and managed at the enterprise level to meet corporate needs in a just-in-time manner, paying for actual use.

5.1.3 IT Infrastructure Portfolio Evolution (HXXB)

It is envisioned that in the near to mid-term (FY 2013-2015) fifty percent of all new IT investments will focus on acquisition of technologies that support VA's "To Be" future workplace. The remaining fifty percent of allocated funds will be spent on sustaining the "As Is" systems and infrastructure where existing users connect via the traditional Campus Area Networks. The long-term (FY 2015-2017) view is for seventy-five percent of technology to be



focused on the “To Be” and twenty-five percent of funds spent on sustainment of “As Is” existing technologies, if doing so proves to be cost effective.¹⁰

VA will use and expand Commodity Enterprise contracts to reduce unit cost to the lowest commercially viable levels. Near-term plans for consolidating IT commodities include:

- Increase VA server virtualization from 50-75% to provide additional capacity for shared services.
- Eliminate analog fax devices and associated maintenance, hardware, and software costs.
- Consolidate mobile device contracts.
- Continue use of PortfolioStat to identify redundant projects and consolidate projects to obtain cost reductions.

Long-term IT Commodity consolidation efforts identified in the OIT FY 2015-2019 Planning Guidance includes increasing investments in the following areas:

- Establish an IT Commodity governance structure to manage key activities in the IT Infrastructure Roadmap.
- Performance Reference Model (PRM) to relate IT systems to business goals and agency functional performance improvement.
- Integrated Priority List (IPL) to establish senior leadership agreement on tasks and activities that consume resources.
- Integrated Master Schedule (IMS) aggregating the schedules and cross-project dependencies for each IPL project.
- Establish an IT Commodity governance structure to manage key activities in the transformation roadmap.
- Coordinate and increase effective implementation of transformation activities.
- Risk Management System to identify material risks for each IPL project, particularly regarding cross-project dependencies, and to identify the scope and impact of each risk.

In addition, OIT recently inventoried its mobile devices and wireless service contracts, and reported the information to OMB for inclusion in the government-wide tool being developed that allows agencies to compare contracting data. A draft of the tool has been released, which VA is sharing with its acquisition community to compare prices and expose them to the soon-to-be-released government-wide contracting tool. The expectation is that VA will be able to negotiate better prices for digital devices and service contracts. VA will continue to update its contract data quarterly and to share its data with all other federal agencies. These measures

¹⁰ VA OIT Information Technology Roadmap, December 5, 2012, Draft 2.14



will allow VA to reallocate more of its requested budget to new development, and shift some investments from maintaining services, while improving service delivery.

5.1.4 IT Cost Optimization

In December 2011, the VA CIO established the RRTF initiative and designated the Deputy CIO for ASD to lead a standing team for ensuring VA pursues all possible options to reduce IT spending. Recommendations for IT reductions are considered for establishment as stand-alone projects with activity and product milestones executed under PMAS and cost avoidance targets expected to be achieved. Below are activities conducted by RRTF to identify opportunities for IT cost savings across VA projects.

- Using expert opinion approaches to examine analytical and engineering processes, perform business case and cost analysis, and re-examine/modify program approaches to reduce historical cost levels
- Reviewing the use of IT equipment, software and systems to determine value, gauge efficiency and formulate recommendations for potential cost avoidance
- Establishing an intake process to continuously solicit and collect ideas and recommendations to improve the efficiency of IT projects and programs, and the acquisition and allocation of equipment
- Examining existing IT requirements and solutions (proposed and actual) for efficiency and potential redundancies across the organization
- Assisting project managers in the development of cost avoidance measures for presentation to the AS/IT

RRTF conducts several operational analyses to identify potential cost containment opportunities. These analyses will provide a data-driven basis for evaluating recommendations for project start up. Current analyses include:

- Sustainment Analysis – Review FY2011 sustainment lines of approximately \$1.6B to produce a cost analysis by spend category and a lifecycle cost analysis of items purchased
- On-Line Analytical Processing (OLAP) Analysis – Analyze current VA analytical reporting (business intelligence) capabilities by identifying data redundancy and poor file and table design practices
- On-Line Transaction Processing (OLTP) Analysis – identify potential redundancy among transaction processing systems in the VA computing environment
- System Inventory – develop a central inventory of systems and applications, including key descriptors of each, to identify candidates for decommissioning

To support eliminating legacy systems, RRTF has established a project, Establish Common Services, to develop and implement a Service Oriented Architecture (SOA) roadmap for the



Veterans Relationship Management (VRM) program. RRTF will also develop a cost analysis for developing and implementing a SOA roadmap. The Establish Common Services project scope includes identifying efficiencies and candidate common services at the enterprise level to enable an accelerated approach to retire outdated legacy components and establish the foundation for enterprise-wide capabilities. If this project is successful, it will be extended enterprise-wide.

RRTF is reviewing the results of an analysis of applications with a low volume of transactions as another potential area for reduced investment.

RRTF is developing a communications plan to increase awareness of RRTF across VA and is considering conducting an OIT Cost Containment Idea Challenge across VA to identify IT cost saving opportunities.

5.2 Enterprise Shared Services (ESS) (HXXC)

VA's Enterprise Shared Services Strategy is a key component of its efforts to provide a Veteran-centric environment as well as to realize efficiencies in its operations. VA is working to provide Service Oriented Architecture (SOA) design patterns that are available for use across the enterprise. SOA is a key capability that will enable OIT to achieve its vision of providing seamless services and information to the Veterans on any device, anywhere, anytime. The strategy will accomplish the following objectives:

- Establish governance and policy and assign responsibilities for the requirement, planning, development, management, and usage of ESS.
- Build shared services compliance into Enterprise Technical Architecture (ETA) policies, specifications, and preferred design patterns.
- Build shared services that are discoverable and re-usable with standard service descriptions that are enterprise-wide discoverable and reusable.
- Promote usage of the authoritative instance of data.
- Manage common capabilities across existing processes and systems.
- Establish training and outreach on VA shared service.
- Promote collaboration with DoD, open source community, and other providers of shared services.



5.2.1 Enterprise Shared Services Target State

The ESS target state depicted in Figure 4 below is derived from the Open Group’s SOA Reference Architecture.¹¹ The Shared Service target state is a combination of the following aspects:

- Organizational Structures, including roles and responsibilities
- Reference Architecture, including key principles, standards, and patterns
- Required Operational Capabilities, including enabling technologies such as Service Taxonomy, Service Registry and Repository, Enterprise Service Bus, Service Definition Framework, Service Versioning, and Service Level Agreement
- Governance, including governing and governed processes; establish working group and sub-groups for Governance, Architecture, Capabilities, and Assessments
- Assess agency Shared Service adoption and maturity through a roadmap concept

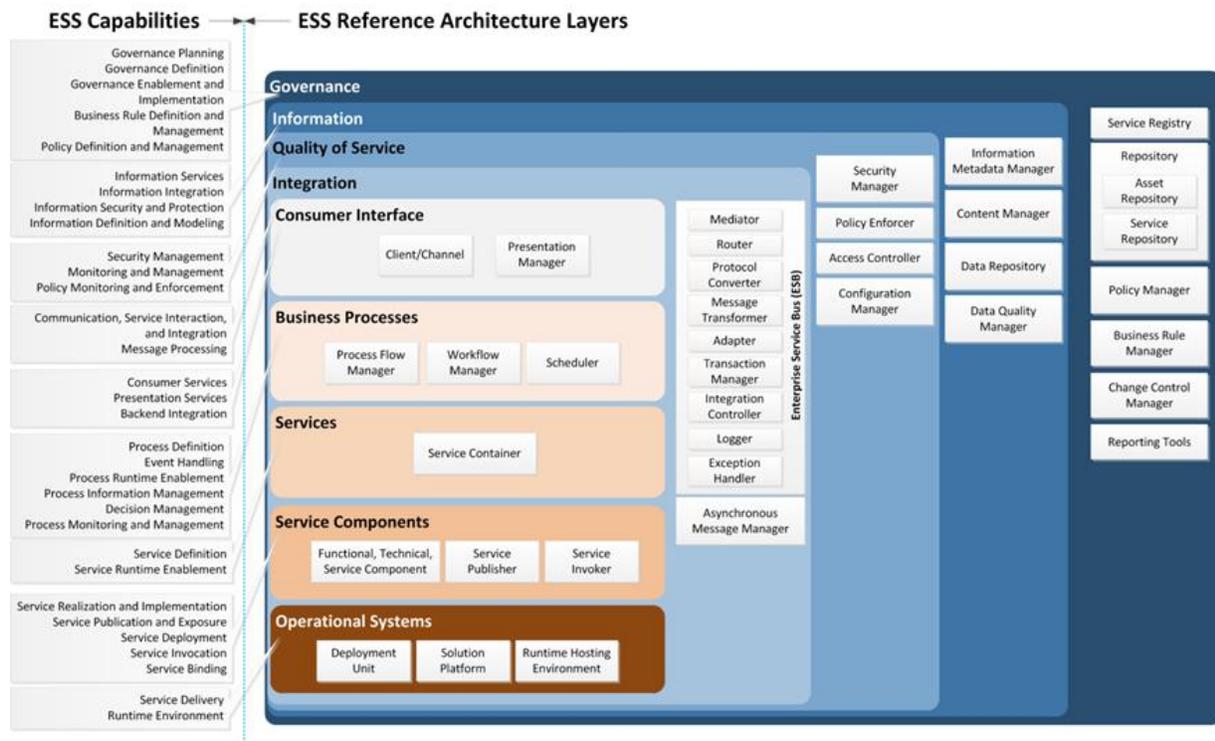


Figure 5: Enterprise Shared Service Reference Architecture

¹¹ The Open Group, SOA Reference Architecture, ISBN: 1-937218-01-0, November 2011



6 Cyber Security, Privacy, and Business Continuity

6.1 Mission and Goals

The Office of Information Security (OIS) within OIT has full responsibility for the VA's data and information security program. OIS provides services, tools, guidance, oversight, and direction to all VA administrations and staff offices. OIS operates under the following mission statement: *"OIS is devoted to supporting care by protecting the personal information of Veterans and the employees who serve them."*

VA is working to ensure that IT investments support Department goals to provide continual improvements in information security. The Department has put in place numerous cybersecurity and privacy measures to support the President's cross-agency goals of continuous monitoring, trusted internet connections, and Homeland Security Presidential Directive 12 (HSPD-12) implementation, and to protect the privacy of personally identifiable information (PII) and sensitive but unclassified (SBU) information.

VA's Security Goals

1. Protect the overall VA information security and privacy posture to ensure confidentiality, integrity, availability, and appropriate destruction of information;
2. Integrate risk and performance management into information security and privacy practices to create a cost- and process -effective program;
3. Establish an Information Security governance structure and policies that create operational efficiency and accountability;
4. Seamlessly integrate security processes into VA's business and IT projects to reduce exposure to risk and maximize efficiency; and,
5. Promote an environment where all employee and contractor actions reflect the importance of information security accountability.

6.2 Security and Privacy IT Investment Alignment (EXXA)

Discussions of cybersecurity investment alignment includes both specific investments in improving VA's core cybersecurity capabilities and ensuring that all VA investments, programs, and initiatives are aligned with and take full advantage of VA's cybersecurity capabilities.

At the forefront of VA's cybersecurity efforts is the ongoing development of an overarching Security Architecture program. It will encompass all layers of the VA enterprise and will be capable of delivering and maintaining desired cybersecurity attributes inclusive of confidentiality, integrity, availability, accountability, and assurance consistent with a "defense in depth" approach.

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 that ensure VA compliance with federal information security and privacy legislation, standard security controls, and VA directives are published in the Enterprise Technical Architecture (ETA) layer of the overall OneVA EA. Adherence is evaluated and verified at each PMAS development milestone. As part of this PMAS development process, all VA IT



capabilities are required to receive full security assessment and authorization prior to initial operating capability (IOC) deployment at Milestone 2. Once deployed, all VA IT capabilities are subject to continuous monitoring with enterprise-wide security enhancements performed throughout the lifecycle by SDE as part of maintenance of the Department's infrastructure capabilities.

To guide and prioritize investments in new VA cybersecurity capabilities, OIS has developed a strategic budget implementation plan. The plan defines OIS's mission, goals, and objectives, which align to the OIT and VA mission, goals, and objectives. Each investment is mapped to these goals and objectives. Investment and portfolio decisions are made based on systematic evaluations and impact rankings against the goals and objectives, ensuring VA compliance with federal information security and privacy legislation, standard security controls and VA directives. To better calculate the benefits of OIS investments and projects, in FY 2012, OIS conducted a comprehensive investment study to serve as a framework for developing a Strategic Investment Tool (SIT).

SIT, along with the data collected in the study, will serve as a basis for analyzing information security/privacy benefits, cross-walking past investments against OIS goals and objectives, baselining current VA organizational maturity based on NIST best practices, and benchmarking VA's risk profile to other federal and commercial entities. Upon implementation of the SIT in FY 2013, the Strategic Portfolio Analysis Tool will enable OIS to select optimal combinations of projects based on organizational maturity, recommend projects within a set annual budget, display Strategic Spend and Benefits impact on strategic goals and objectives, and assist in planning and benefit aggregation for multi-year projects.

6.3 Security and Privacy Services

6.3.1 Continuous Readiness in Information Security

OIS supports the Continuous Readiness in Information Security Program (CRISP), the new operating model to improve the information security implementation across each level of the cyber architecture. Through this program, VA has either initiated or completed enterprise-wide actions addressing security management, segregation of duties, access controls, contingency planning, and configuration management. This has allowed VA to address many of its outstanding Plans of Actions and Milestones (POAMs) and has resulted in significant remediation of many of the deficiencies that compromise its material weakness in IT security controls.

6.3.2 Continuous Monitoring

As part of its continuous monitoring program, OIS completed the first two phases of the Visibility to Everything initiative (V2E). Critical data delivered by the V2E project during FY 2012 has significantly increased the visibility of devices, servers, voice and video devices, layer 2/3 network interfaces, and wireless Local Area Network controllers, firewalls, routers, switches



and Wide Area Network traffic optimizers. In addition to facilitating visibility to all endpoints (over 370,000), it addresses vulnerabilities discovered on those machines. As a part of this visibility, extensive near-real-time reporting and cybersecurity analysis is available to generate executive dashboard summaries, reporting artifacts, and reporting requests to meet customer requirements. The analysis and visibility result in a feedback loop that reviews, analyzes, and recommends remediation and re-architecting initiatives to the existing VA Security Architecture. Planning is underway with VHA Biomedical Engineers to add tools to use the same network for monitoring the Medical Device Information Architecture (MDIA). In late FY 2012, OIS began integration of the Governance, Risk, and Compliance (GRC) tool to incorporate prior Visibility to Desktop feeds, Visibility to Server feeds, and other VA security tools into one graphical dashboard. In FY 2013, the tool will be leveraged during the Assessment and Authorization (A&A) process and will provide information used to determine the security posture of the Department.

6.3.2.1 HSPD-12 Implementation

VA has enabled almost all of its more than 350,000 user devices with Smartcard capabilities, and has issued Personal Identity Verification (PIV) cards to most of its employees and contractors. Currently, approximately 5,000 VA employees and contractors that work in VA's Central Office campus are required to log into the VA network using their PIV card while on campus. Plans are in place to require PIV card-based logical access throughout the enterprise.

6.3.2.2 Trusted Internet Connection/Einstein

National Cybersecurity Protection System (NCPS; formerly known as Einstein) devices are deployed in all four VA Trusted Internet Connection (TIC) Gateways. VA has met 82% of TIC 2.0 critical requirements with a robust toolset comprising a fully operational set of protective measures. The remaining 18% primarily pertain to administrative and management controls. VA remains committed to the implementation of all critical requirements.¹² VA will establish a TIC and seek authority to operate as a TIC Access Provider (TICAP) for VA Internet access. The TIC Service Center will meet all federal requirements for TIC service providers and will utilize VA's four Internet gateways (Reston, Virginia, Dallas, Texas, Chicago, Illinois, and San Jose, Puerto Rico) to establish the TICs. The implementation of TIC will improve the security of VA's enterprise network by instituting common security controls and configurations as well as installing additional monitoring capabilities.

¹² VA Office of Information Security 2012 Annual Report



6.3.3 Securing Personal and Sensitive Information (GXXB)

VA provides information protection, including protection for all personal information (e.g., PII) and controlled, unclassified information (CUI), in three ways:

1. *Confidentiality* – information is made available only to those who rightfully have a need-to-know and should have access
2. *Integrity* – information is modified only by those who are authorized to do so
3. *Availability* – information is accessible only to those who need to know and are authorized to receive it when they need it

To ensure the privacy and security of Veterans' data, their beneficiaries, VA's employees, and other stakeholders, VA has implemented policy and training to ensure that VA systems are compliant with NIST Special Publication 800-53 controls for federal systems, as well as with additional VA-specific security controls. Further, VA, like other federal agencies, is working to develop and implement its Department-level CUI program and the frequency of controls verification.

6.3.3.1 Policy

VA Handbook 6500, Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program and Handbook 6500.2, Management of Data Breaches Involving Sensitive Personal Information (SPI), informs VA personnel of requirements related to suspicion of a privacy breach, responsibilities for identifying security requirements, and the appropriate level of security controls for information system(s) where SPI is currently created, collected, processed, disseminated, stored, or subject to disposal. It also states instructions for remote access to VA information systems and requirements for program managers regarding employee and contractor access to VA information and/or systems.

VA Directive 6609, Mailing of Personally Identifiable and Sensitive Information, provides procedures for the mailing of PII and other SBU, and requires that audit and event logs generated by VA IT systems be reviewed by the Incident Resolution Team (IRT) and reported to the Data Breach Core Team (DBCT) and the CIO.

Lastly, VA Directive 6508, Privacy Impact Assessments and accompanying VA Handbook 6508.1, Privacy Impact Assessment (PIA), states requirements for assessment of risks associated with the collection, use, and dissemination of PII.

6.3.3.2 Training, Awareness, and Outreach

VA employees, contractors, and volunteers with access to VA information systems or paper information containing PII or SBU are informed and reminded of their roles and responsibilities through completion of mandatory annual privacy and security training. In addition, National Rules of Behavior must be reviewed and accepted before access to any VA information system can be granted.



6.3.3.3 Information Security

VA systems are compliant with NIST Special Publication 800-53 controls for federal systems, as well as with additional VA-specific security controls. Other measures to ensure appropriate account management include automated mechanisms to audit account creation, modification, disabling and termination actions, and appropriate notification as required.

6.4 Business Continuity (EXXB)

OIT's approach to Business Continuity is a five stage process known as the Information System Contingency Plan Assessment (ISCPA).¹³

Stage 1: Identifies and maps OIT information system contingency planning requirements through development of a business impact analysis (BIA), threat assessment, and vulnerability assessment.

Stage 2: OIT strategy determination; generation of Information System Contingency Plans (ISCPs) and Disaster Recovery Plans (DRPs)

Stage 3: Places the plans in the appropriate OIT repository followed by document review and approval

Stage 4: Training OIT operations staff in ISCP and DRP roles and responsibilities; exercising individual components of plans; plan validation through testing, and updating plans as necessary

Stage 5: Placement of OIT test results, updates, and validated plans in the approved repository

¹³ VA Directive 0323, VA Continuity Program, November 5, 2010



7 Workforce Development and Accessibility

7.1 Competency Models and Diversity (FXXA, IXXA)

OIT IT Workforce Development (ITWD) supports and implements competency models across OIT to ensure a fully trained IT workforce capable of meeting VA's strategic goals and objectives. The VA competency models build on the Office of Personnel Management Information Technology Roadmap and are customized to reflect the specific needs of VA OIT. OIT competency models provide employees with a framework that sets the baseline of knowledge, skills, and abilities for IT roles. These models, shown in Figure 6, also identify training needs for professional development and support OIT's overall efforts to build a future ready workforce.

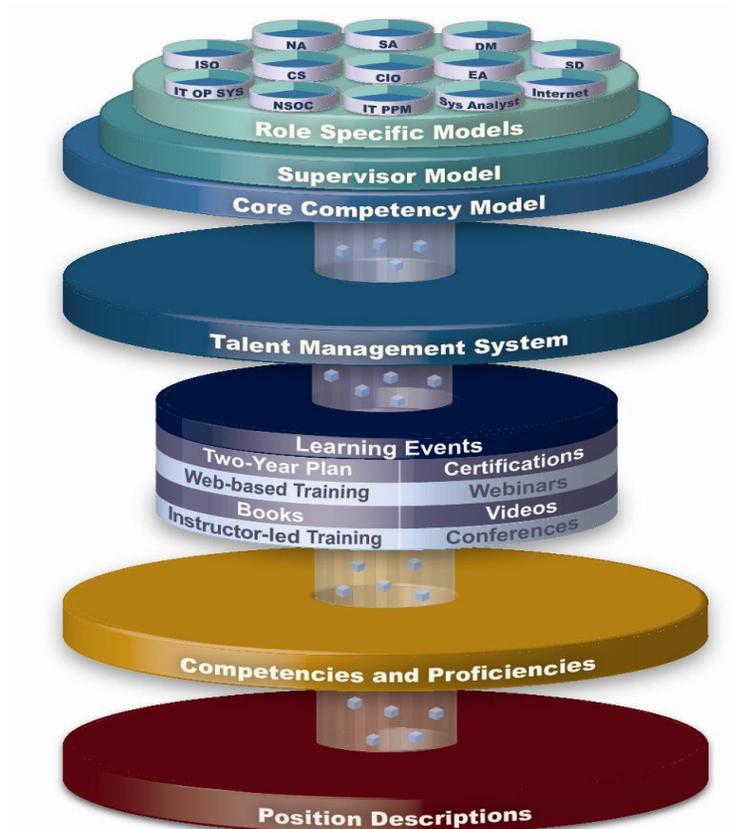


Figure 6: Competency Model Overview

By using the competency models, supervisors create a strategic and tactical career development plan with their employees. The career development plan is customized to balance the needs of the employee with the most critical strategic direction needed at the time for VA. OIT promotes diversity and professional development through the competency model process. The competency models help employees determine skill gaps in order to create



tangible professional development paths to follow throughout their careers, developing their skills and abilities. The competency models are used to organize the courseware in VA Talent Management System (TMS) on-line education training systems. OIT ITWD will continue to add a variety of up-to-date training events to each competency, in each job role, and at each proficiency level, in order to ensure that relevant and current training is always available.

All OIT supervisors and leaders are assigned competencies that foster an inclusive environment, such as Leveraging Diversity and Developing Others. Leaders are expected to possess these competencies at a proficiency level appropriate to executing their jobs successfully. Resources available to teach leaders how to create a diverse environment include the Performance Management webinar series, the Supervisor's Reference Library, the Programming with Section 508 In Mind webinar series, and the Basic Elements of Supervision Training (BEST) curriculum. OIT, through recurring competency gap analysis, will refine and develop emerging training strategies to minimize identified gaps and remain agile in our transformational environment.

OIT is committed to providing professional certification opportunities to the VA IT workforce. These programs increase the knowledge, skills, and abilities of IT staff and directly impact the level and quality of service OIT provides in support of Veterans. ITWD manages a comprehensive catalog of IT certification offerings that includes Certified Information System Security Professions, CompTia Security +, CompTia Network +, and Certified Ethical Hacker. Additionally, OIT has mandated Federal Acquisition Center Program-Project Manager (FAC P-PM) certification for all IT program and project managers executed in partnership with the VA Acquisition Academy.

OIT supports a diverse workforce and provides accessible applications and systems by researching and suggesting hardware, software, and assistive technology for its disabled workforce. VA ensures that their 28,000 disabled employees have access to and use of information and data comparable to that of non-disabled VA employees unless an undue burden would be imposed on the Agency.

7.1.1 OIT Workforce Strategic Alignment (FXXA)

OIT is performing two human capital planning phases to support the future workforce that will also support the Department's strategic goals and objectives. The first phase is the establishment of an interim stand-alone OIT Human Capital Management Strategic Plan (HCMSP). Our plan will encompass a full strategy development process, which will be led by the OIT Human Capital Strategic Working Group (HCSWG). The HCSWG is mentored and guided by VA's Office of Human Resources Management Office of Workforce Planning (HRMOWP), which recently drafted the VA Human Capital Plan for FY 2013-2017. The HRMOWP assisted the HCSWG in developing the initial framework, which will drive all strategic planning to ensure that the OIT HCMSP is linked to VA's Strategic Plan, VA agency goals and objectives, and the performance measures and milestones as outlined in the Human Capital Assessment and Accountability Framework (HCAAF). Additionally, the HCMSP will be synchronized with OIT



subordinate organization human capital goals and objectives. The ultimate goal is the production of the OIT Human Capital Strategic Plan for FY 2014-2016 by September 30, 2013.

The second phase is the participation and coordination activities related to the FY 2015-2019 OIT Strategic Plan. In January 2013 the core planners from the HCSWG participated in the OIT Planning Guidance Lockdown, which resulted in the establishment of planning guidance for OIT. The HCSWG ensured that necessary aspects of OIT Human Capital Management Strategic Planning were incorporated into the OIT Planning Guidance.

7.2 Workforce Accessibility and 508 Requirements (IXXB, IXXC)

OIT leadership understands the importance of adhering to Section 508 accessibility requirements and guidelines when IT systems and tools are developed, procured, and maintained. The VA's overall strategy for accessibility is incorporated in VA's policies, outreach and awareness, and measurable deliverables.

The following identifies how VA currently integrates accessibility and Section 508 considerations into processes used in developing, procuring, maintaining, and generally using IT solutions.

- **Software Development** – Section 508 artifacts are built into ProPath for Project Build to ensure software development adheres to Section 508 Program Office standards. ProPath was established in order to enhance and encourage standard, repeatable processes that can be utilized easily across the organization and is the first step in a long-term investment toward improving our development processes.
- **Acquisitions** – OIT is committed to extended accessibility into the acquisitions process. Section 508 Program Office reviews IT Acquisition Request System (ITARS) submissions to ensure Section 508 contract language is embedded in the acquisitions.
- **Workforce Development and Training** – OIT works closely with VA's Section 508 Program Office to develop and offer Section 508 training. OIT has collaborated with VA subject matter experts to develop a webinar called "Programming with Section 508 In Mind." Additionally, employees have access to over 60 accessibility- and Section 508-related learning activities when they are building their Individual Development Plans. OIT will continue to refine and enhance the training that is available, so employees have access to the latest Section 508 requirements and guidelines. In addition, OIT ensures that employees are aware of accessibility considerations through the OIT competency model. The competency *Accessibility* or "the knowledge of tools, equipment, and technologies used to help individuals with disabilities use computer equipment and software," is included across many of the competency models. OIT employees are assigned this competency and are expected to meet specified proficiency targets.
- **Conformance Audits** – The Section 508 Program Office performs Section 508 conformance audits and offers remediation planning assistance as required.



Appendix A VA 2013-2015 Enterprise Roadmap



Acronyms

Acronym	Definition
A&A	Assessment and Authorization
ASCI	American Satisfaction Customer Index
APG	Agency Priority Goal
ASD	Architecture, Strategy, and Design
AS/IT	Assistant Secretary for Information and Technology
BEST	Basic Elements of Supervision Training
BIA	Business Impact Analysis
BNTIB	Budgeting and Near Term Investment Board
BOP	Business Operating Plan
CA	Customer Advocate
CCD	Continuity of Care Document
CDI	Content Data Initiative
CDM	Conceptual Data Model
CFO	Chief Financial Officer
CIO	Chief Information Officer
CRISP	Continuous Readiness in Information Security Program
CUI	Controlled, Unclassified Information
DAP	Digital Analytics Program
DBCT	Data Breach Core Team
DRPs	Disaster Recovery Plans
DoD	United States Department of Defense
EA	Enterprise Architecture
eCFT	Electronic Case File Transfer
ELDM	Enterprise Logical Data Model
EMF	Enterprise Management Framework
ePMO	Enterprise Program Management Office
ERM	Enterprise Risk Management
ESS	Enterprise Shared Services
ETA	Enterprise Technical Architecture
EVH	Eliminate Veteran Homelessness
FDGS	Federal Digital Government Strategy
FOIA	Freedom of Information Act
GSA	General Services Administration
GRC	Governance, Risk, and Compliance
HCAAF	Human Capital Assessment and Accountability Framework
HCMSP	Human Capital Management Strategic Plan



Acronym	Definition
HCSWG	Human Capital Strategic Working Group
HRMOWP	Human Resources Management Office of Workforce Planning
HSPD-12	Homeland Security Presidential Directive 12
IAM	Identity and Access Management
ICH	Interagency Council on Homelessness
iEHR	Integrated Electronic Health Record
IPL	Integrated Priority List
IRM	Information Resources Management
IRT	Incident Resolution Team
ISCPA	Information System Contingency Plan Assessment
ISCPs	Information System Contingency Plans
ISO	Information Security Officers
IT	Information Technology
ITARS	IT Acquisition Request System
ITLB	Information and Technology Leadership Board
ITRM	IT Resource Management
ITWD	IT Workforce Development
LAN	Local Area Network
MDIA	Medical Device Information Architecture
MYP	Multi-Year Planning
NaaS	Network as a Service
NIST	National Institute of Standards and Technology
OIS	Office of Information Security
OIT	Office of Information and Technology
OMB	Office of Management and Budget
OPP	Office of Policy and Planning
OSHA	Occupational Safety and Health Administration
PD	Product Development
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PLTIB	Planning and Long Term Issues Board
PMAS	Project Management Accountability System
PMTF	Process Methodology Task Force
POAMs	Plans of Actions and Milestones
PPBE	Planning, Programming, Budgeting/Execution and Evaluation
PTSD	Post Traumatic Stress Disorder
QPO	Quality, Performance and Oversight
RRTF	Ruthless Reduction Task Force



Acronym	Definition
SBU	Sensitive But Unclassified
SDE	Service Delivery and Engineering
SIT	Strategic Investment Tool
SMC	Strategic Management Council
SOA	Service Oriented Architecture
SPI	Sensitive Personal Information
SRG	Senior Review Group
TIC	Trusted Internet Connection
TICAP	Trusted Internet Connection Access Provider
TMS	Talent Management System
UFR	Unfunded Requirement
V2E	Visibility to Everything
VA	United States Department of Veterans Affairs
VAEB	VA Executive Board
VBMS	Veterans Benefits Management System
VHA	Veterans Health Administration
VLER	Virtual Lifetime Electronic Record
VRM	Veterans Relationship Management



Bibliography/References

1. The Open Group, SOA Reference Architecture, ISBN: 1-937218-01-0, November 2011.
2. VA, CIO Annual Report FY 2012 (DRAFT).
3. VA, Directive 0323, VA Continuity Program, November 5, 2010.
4. VA, Directive 6051 "VA Enterprise Architecture (EA)," July 12, 2002.
5. VA, IT Strategic Plan FY 2006-2011, December 2007.
6. VA, Memorandum, "Office of Information and Technology (OIT) Fiscal Year (FY) 2015-2019 Planning Guidance," March 12, 2013.
7. VA, Office of Information Security 2012 Annual Report.
8. VA, OIT Information Technology Roadmap, December 5, 2012 (DRAFT).
9. VA, PAID Human Resources Data, dated March 31, 2013.
10. VA, PortfolioStat 2012 Overview, Government Accountability Office (GAO) briefing, April 11, 2013.
11. VA, Strategic Plan Refresh FY 2011-2015.