



Department of Veterans Affairs
FY 2013-2015 Information Resources
Management Strategic Plan

Office of Information and Technology

March 28, 2014



Table of Contents

Letter from the Deputy Secretary	1
Executive Summary	2
Introduction	4
Background	6
1 VA Strategic Goals, Objectives, and Priorities	8
1.1 VA Strategic Goals, Objectives, and Agency Priority Goals (AXXA)	8
1.2 OIT Mission, Vision, Strategic Goals, and Priorities.....	10
1.3 Relationship between VA Strategic Planning and IT Strategic Planning (AXXB, CXXD).....	15
2 Chief Information Officer Roles, Responsibilities, and Organization (DXXA)	20
2.1 Office of Information and Technology	20
3 Governance and Management Processes	25
3.1 VA Executive Governance.....	25
3.1.1 VA Executive Board (VAEB) (CXXB, CXXD).....	25
3.1.2 Strategic Management Council (SMC)	25
3.1.3 Senior Review Group (SRG).....	26
3.2 IT Governance, Investment, and Portfolio Management (CXXA).....	26
3.2.1 IT Leadership Board (ITLB)	26
3.2.2 IT Planning, Programming, Budget and Execution Board (IT PPBEB).....	26
3.3 Project Management Accountability System (PMAS) (CXXE, CXXF).....	27
3.4 Enterprise Risk Management (ERM)	28
3.5 IT Process Asset Library	28
3.6 Evolving VA Corporate Enterprise Processes (CXXC, CXXD)	29
3.6.1 Planning, Programming, Budgeting, and Execution (PPBE)	29
3.6.2 Acquisition Program Management Framework (APMF).....	30
3.6.3 End-to-End Requirements Management (E2ERM)	31
4 Mission Capabilities – Creating a “Veteran-Centric” VA (GXXA, BXXA, BXXC)	32
4.1 Open Government.....	34
4.1.1 The Open Data Initiative	34
4.1.2 Federal Digital Government Strategy Initiative	35
4.2 Secure Mobile Applications (BXXB)	36
4.3 Managing Information as an Asset (GXXA).....	38
4.3.1 Integrated Electronic Health Record (iEHR).....	38
4.3.2 Identity and Access Management (IAM).....	39
4.3.3 Customer Data Integration (CDI)	40
4.3.4 Architecture	41



5	IT Infrastructure Optimization	42
5.1	Maturing the IT Portfolio (HXXA).....	44
5.1.1	Strategic IT Sourcing Plan (CXXG).....	44
5.1.2	Enterprise Licensing (CXXG)	45
5.1.3	IT Infrastructure Portfolio Evolution (HXXB).....	45
5.1.4	IT Cost Optimization.....	46
5.2	Enterprise Shared Services (ESS) (HXXC)	48
5.2.1	Enterprise Shared Services Target State	48
6	Cyber Security, Privacy, and Business Continuity	50
6.1	Mission and Goals.....	50
6.2	Security and Privacy IT Investment Alignment (EXXA)	50
6.3	Security and Privacy Services.....	51
6.3.1	Continuous Readiness in Information Security.....	51
6.3.2	Continuous Monitoring	52
6.3.3	Securing Personal and Sensitive Information (GXXB)	53
6.4	Business Continuity (EXXB).....	54
7	Workforce Development and Accessibility	55
7.1	Competency Models and Diversity (FXXA, IXXA).....	55
7.1.1	OIT Workforce Strategic Alignment (FXXA)	56
7.2	Workforce Accessibility and 508 Requirements (IXXB, IXXC).....	57
	Appendix A VA 2013-2015 Enterprise Roadmap	58
	Appendix B: OMB M-13-09 Reporting Codes	59
	Acronyms.....	62
	Bibliography/References	64



Letter from the Deputy Secretary

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

VA's *Information Resources Management (IRM) Strategic Plan* and accompanying *VA Enterprise Roadmap* reflect that commitment to enterprise-wide transformation. VA is moving to a people-centric, results-driven, and forward-looking organization that is focused on serving Veterans in a comprehensive and proactive manner. While these documents highlight programs and budgets for Fiscal Year (FY) 2014-2015, the decisions reflected align with the VA Strategic Goals for FY 2014-2020. VA's FY 2014-2020 goals and objectives shift focus from improvements within a service or benefit delivery program to coordination and integration across programs and organizations, measuring performance by the ultimate outcome for the Veteran, and putting the Veteran in control of how, when, and where they wish to be served.² Different information technology capabilities and IT infrastructure are required to support VA's strategic goals and objectives.

The development of this *VA IRM Strategic Plan* and *VA Enterprise Roadmap* are the result of a collaborative effort among VA Administrations and staff offices, and in particular the Office of Information and Technology (OIT) and the Office of Policy and Planning (OPP) that are tasked with using data-based decisions to increase integration across the enterprise.

This *VA IRM Strategic Plan* and *VA Enterprise Roadmap* provide a comprehensive view of VA transformation in a consolidated format previously unavailable. By making this information available to Veterans, VA employees, our partners, and the public, it is our hope that all our stakeholders better understand VA's vision, goals, and plans to improve service to our Veterans.

Sloan D. Gibson
Deputy Secretary of Veterans Affairs

¹ *VA Strategic Plan FY 2014-2020*, March 6, 2014

² *Ibid*, pg., 24.



Executive Summary

This *VA Information Resources Management (IRM) Strategic Plan* describes how VA governs information technology (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. This *FY 2013-2015 VA IRM Strategic Plan* reflects how VA is strengthening processes—including strategic planning—and improving Enterprise Architecture (EA) to guide transformation. The accompanying *VA Enterprise Roadmap* provides greater detail to the transition plans of each of the Administrations and the Office of Information and Technology (OIT). Together, these plans describe activities for utilizing IT resources to effectively and proactively meet VA's mission to serve the Nation's Veterans and their families. Both plans are living documents that will change to continually reflect VA's progress as it executes programs and measures results.

Achieving a Veteran-Centric Environment

VA is moving to a Veteran-centric environment focused on serving Veterans in a comprehensive, proactive manner—to provide Veterans with high-quality and efficiently delivered benefits and services. To achieve that environment, as articulated in VA strategic goals and objectives and Agency Priority Goals (APGs), and guided by the VA Chief Information Officer's (CIO's) goals, objectives and priorities, the supporting information environment is moving from disparate stovepiped processes and systems to a unified environment of integrated, interoperable business processes and technical services. Through this transformation, VA will shift focus from making improvements within a service or benefit delivery program to coordinating and integrating across programs and organizations. From this mission-centric perspective, VA will measure performance by the ultimate outcome for the Veteran, and put the Veteran in greater control of how, when, and where they wish to be served.

Integration of VA's core processes and information is necessary to achieve this environment. IT Strategic Planning, Programming, Budgeting, and Execution (PPBE) and Reporting activities, for instance, provide critical inputs to VA-decision-making, and support outputs reported to the Office of Management and Budget (OMB) through the PortfolioStat reporting process. The evolution and maturation of VA's processes will produce related evolution and maturation in the *VA IRM Strategic Plan* and *VA Enterprise Roadmap* that reflect both VA's current state and the vision for the way ahead.

How to Use the *VA IRM Strategic Plan*

The *VA IRM Strategic Plan* is a key strategic artifact that contains valuable information for use by leadership at multiple levels across VA. Table 1 provides a short description of the specific purpose and use of the *VA IRM Strategic Plan* for various VA leader positions.



Table 1 - Purpose and Use of the VA IRM Strategic Plan by VA Position

Position	VA IRM Strategic Plan Purpose and Use
VA Secretary VA Deputy Secretary VA Chief of Staff	Provide an overview of VA-wide information resource management which confirms how OIT ensures investments and activities align to and support VA strategic goals and objectives
VA Chief Information Officer	Documents CIO authorities and IT governance
VA Chief Technology Officer	Provides understanding of VA IT authorities and processes that govern IT investments and technology evolution
VA Chief Human Capital Officer	Provides an understanding of desired competencies and personnel development needed to support VA-wide transformation
VA Chief Financial Officer and IT Chief Financial Officer	Provides an understanding of VA's IT investment governance and processes to verify alignment to VA strategic goals and objectives
VA Chief Acquisition Officer	Provides an understanding of information resource management content and processes to ensure acquisition strategies are optimized to leverage the full value of IT investments
VA Performance Improvement Officer	Provides an understanding of IT investments to support performance measures as evidence of IT alignment to and support of VA strategic goals and objectives
VA Administration and Staff Office Executive Leaders	Provides an understanding of information resource management processes and investments to ensure they are appropriately informed by VA business needs
IT Executive Leaders	Ensure information resource management processes and investment needs are appropriately informed by and reflect infrastructure needs to maximize support of VA strategic goals and objectives
IT Managers	Ensure IT program and project needs are appropriately informed and aligned to support VA strategic goals and objectives
VA Chief Enterprise Architect	Provides an understanding of the information resource management processes in order to inform and establish the right EA business rules, standards, and processes to provide appropriate enterprise architecture analyses and artifacts that support senior level decision making



Introduction

About the Department of Veterans Affairs (VA)

With a workforce of over 340,000 employees, VA provides a wide array of benefits and services to Veterans and their beneficiaries. VA health care facilities include 151 Medical Centers, 820 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 [along with education, housing, vocational rehabilitation and insurance] to nearly four million Veterans and beneficiaries, supports 56 Regional Benefits Processing Offices, and maintains 131 National Cemeteries while supporting 90 State or Tribal Cemeteries as national shrines.³

The IT capabilities and services to support this scale of service delivery to Veterans are significant. VA's annual information technology investment of \$3.68B⁴ is a significant contributor to sustaining effective provision of benefits and services to Veterans and their beneficiaries. With such a large investment, VA must exercise stewardship to effectively plan and execute the budget and to ensure proper alignment with mission priorities. 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 361,000 desktop computers, 38,000 laptops, 24,000 mobile devices, and 548,000 email accounts. The OIT government workforce is made up of approximately 7,900 employees. OIT's stewardship of VA's IT budget is critical for ensuring that dollars are managed effectively and business needs are met.

About this VA Information Resources Management Strategic Plan

This *VA IRM Strategic Plan* (including the accompanying *VA 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 CIO, supported by the Office of Architecture, Strategy, and Design (ASD), is responsible for the *VA IRM Strategic Plan*. Developing this *IRM Strategic Plan* is a collaborative effort among many offices across VA working together.

The *VA IRM Strategic Plan* for FY 2013–2015 is VA's first iteration of an IRM Strategic Plan based on OMB's new reporting requirements. The *VA IRM Strategic Plan*, together with the *VA Enterprise Roadmap*, provides an integrated, comprehensive view of the Department's overall transformation. Additionally, development of the *VA IRM Strategic Plan* and *VA Enterprise Roadmap* are closely tied to development of the *VA Strategic Plan*. The relationship among these

³ *VA Strategic Plan FY 2014-2020*, March 6, 2014

⁴ VA OIT FY 2014 President's Budget



documents is shown below in Figure 1. The figure illustrates how the *VA Enterprise Roadmap* is an appendix to both the *VA Strategic Plan* and the *VA IRM Strategic Plan*.

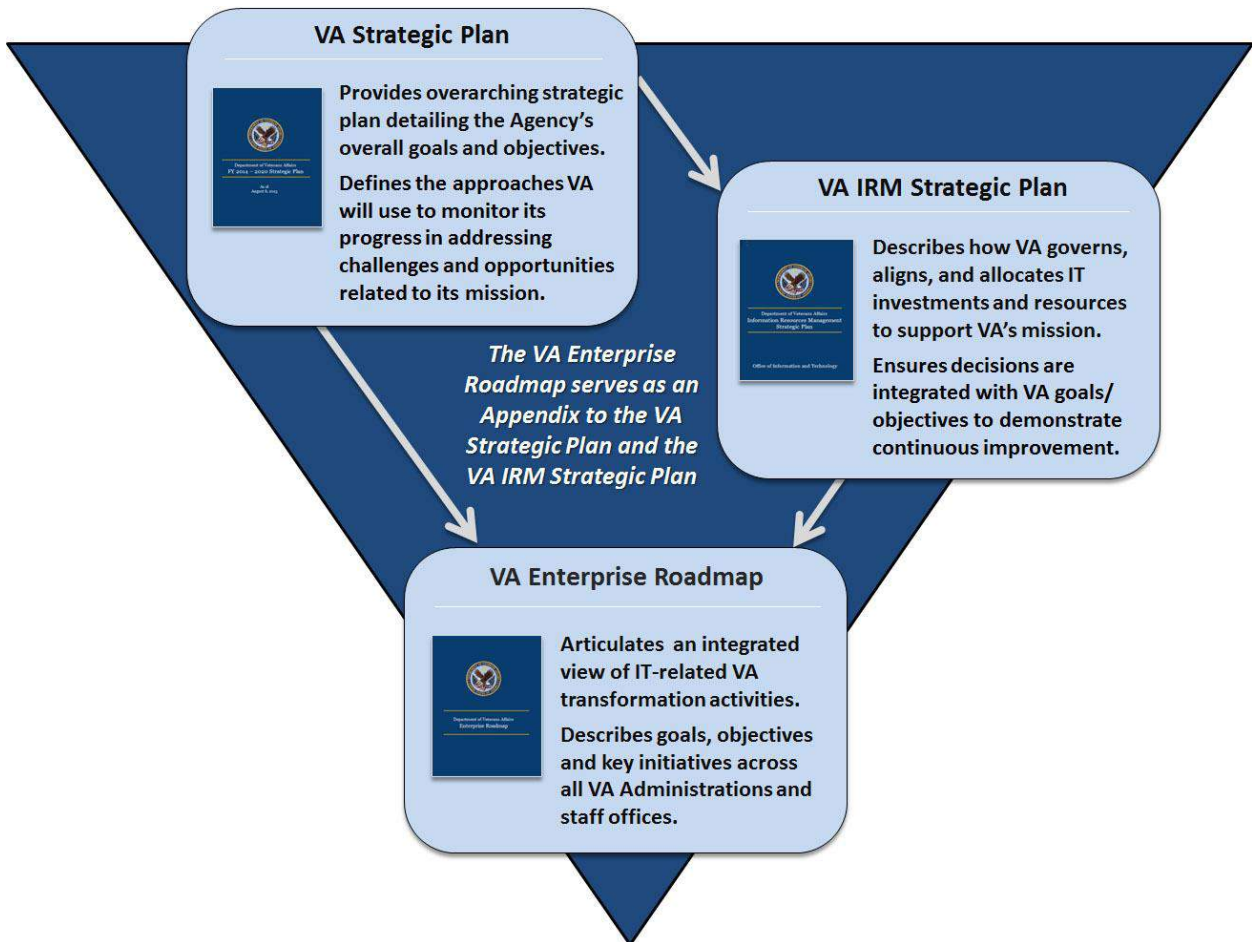


Figure 1 – Relationship among Key Strategic Planning Documents



Background

VA's information resources management efforts are supported by OMB's PortfolioStat effort. PortfolioStat is an OMB-led effort to understand how the government can use IT to better meet business and mission needs. OMB designed PortfolioStat as a tool for agencies to use to assess the maturity of their IT portfolio management process, make decisions on eliminating duplication, augment current CIO-led Capital Planning and Investment Control (CPIC) processes, and move to shared solutions in order to maximize the return on IT investments across the portfolio. PortfolioStat examines the portfolio as a whole and draws on the agency's EA to help identify and eliminate areas of duplication and waste.⁵

OMB PortfolioStat puts particular emphasis on assessing VA's adoption of the following best practices for maturing management of IT resources:⁶

1. Empowering Agency CIOs through a strong partnership between program and mission officials
2. Strengthening IT portfolio governance through the use of effective investment review boards (IRBs) including the use of enterprise architectures and valuation methodologies
3. Advancing service delivery through means such as cloud computing for a more scalable and transparent way to provide IT services

To improve the outcomes of PortfolioStat and advance agency IT portfolio management, OMB is consolidating previously collected IT plans, reports, and data calls into three primary collection channels. The first two are IRM Strategic Plans and Enterprise Roadmaps. The third is called Integrated Data Collection that, along with related quarterly meetings, is often referred to as PortfolioStat.⁷ Sections of the *VA IRM Strategic Plan* that meet specific content requirements from OMB are indicated by a four-letter code, such as AXXA. A complete list of the OMB codes and their associated requirements is provided in Appendix B.

Table 2 delineates approaches that VA has established to better: (1) monitor and account for IT deliverables through incremental and Agile development (i.e., delivering IT functionality in increments of 6 months or less); (2) strategize on where to avoid excessive cost and become more efficient by identifying wasteful, low-value and duplicative IT projects; and (3) consolidate IT. These approaches also support the Department's ability to satisfy OMB PortfolioStat requirements.

⁵ OMB Memo M-12-10, *Implementing PortfolioStat*, March 30, 2012

⁶ OMB Memo M-13-09, *Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management*, March 27, 2013

⁷ Ibid



Table 2 - VA Established Approaches to PortfolioStat⁸

Approaches Implemented	Objectives
IT Investment Governance Boards	<ul style="list-style-type: none">• Provide framework for decision-making and accountability required to ensure IT initiatives meet strategic and business objectives of the Department in an efficient and effective manner• Facilitate executive oversight of all VA's IT initiative planning and management• Advise CIO and Administration Senior Leadership of IT portfolio/program status
Project Management Accountability system (PMAS)	<ul style="list-style-type: none">• Tracks all VA IT projects for adherence to a 6 month milestone policy• Requires program management reviews with OIT and Administration Senior Leadership to provide early identification of projects with high risk flags
Ruthless Reduction Task Force (RRTF)	<ul style="list-style-type: none">• Proposes Department-wide cost reduction strategies• Identifies areas where the Department can reduce excessive costs and become more efficient• Recommends elimination of wasteful, low-value or duplicative IT projects
Accountability Efforts	<ul style="list-style-type: none">• Execute PMAS• Monitor and act upon actions in various management reports, such as Rigor and Performance (RAP) report, Operational and Program Management Reviews• Incorporate suggestions from Customer Satisfaction Surveys, Administration Leadership, and business process point of contacts (POCs)
Budget Operating Plan Management	<ul style="list-style-type: none">• Utilizes IT governance boards' prioritization efforts to implement business requirements• Identifies unfunded requirements for consideration in budget deliberations

⁸ VA IT Portfolio Management Process Maturity Overview, PowerPoint presentation, June 12, 2012



1 VA Strategic Goals, Objectives, and Priorities

VA’s FY 2014-2020 Strategic Plan establishes three strategic goals that are statements of what VA wants to achieve to advance the Department’s mission and address challenges and opportunities. In addition, the VA FY 2014-2020 Strategic Plan reaffirms the Department’s commitment to achieve the three FY 2015 APGs that represent the Secretary’s highest priorities for short-term, high-impact improvement in VA mission performance.⁹

1.1 VA Strategic Goals, Objectives, and Agency Priority Goals (AXXA)

The VA FY 2014-2020 Strategic Plan builds on the prior strategic plan (VA Strategic Plan FY 2011-2015) to continue the significant transformation of VA operations. The VA FY 2014-2020 Strategic Plan places a stronger emphasis on defining success by Veteran outcomes; enhancing the quality of and access to benefits and services through integration within VA and with our partners; and developing the skills, tools, and leadership of the VA workforce to meet client needs and expectations. VA’s strategic goals and objectives are depicted in Figure 2.

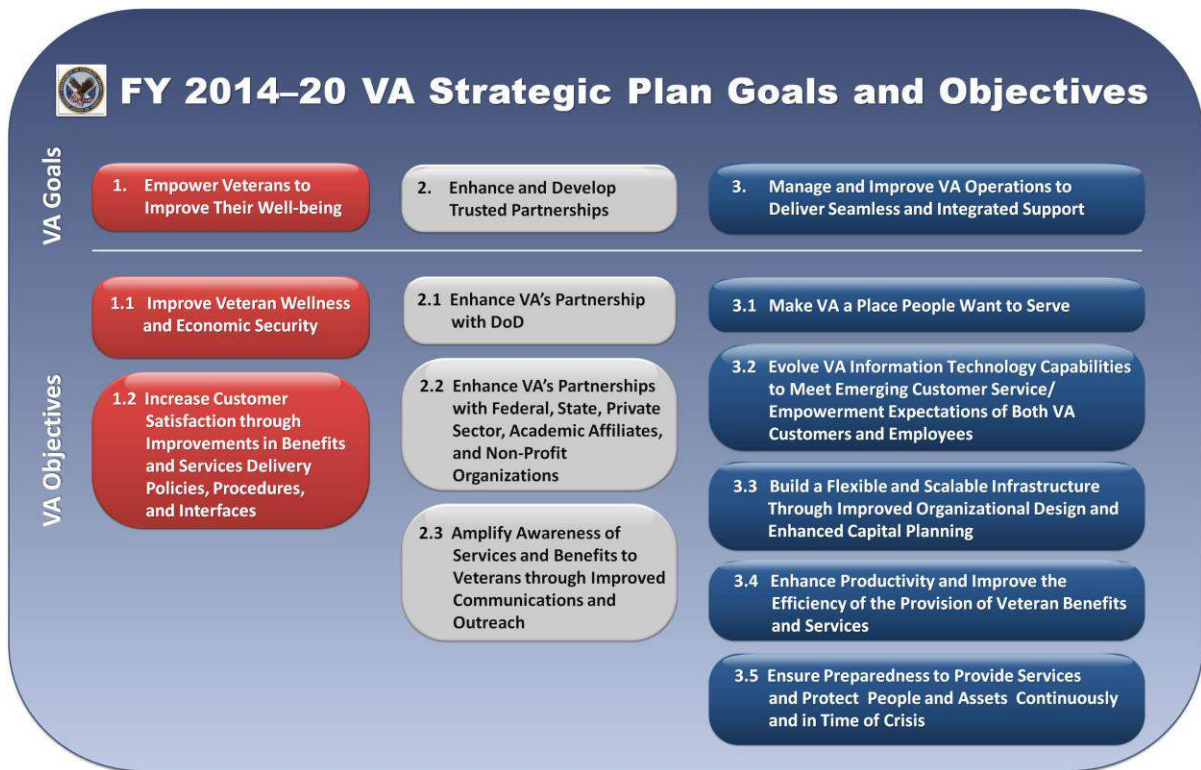


Figure 2 – VA FY 2014-2020 Strategic Goals and Objectives¹⁰

⁹ VA Strategic Plan FY 2014-2020, March 6, 2014

¹⁰ VA Programming Guidance Fiscal Year 2016-2020 PPBE Cycle, October 2, 2013



Each of VA's three strategic goals is broken down into a set of objectives that express more specifically how VA will achieve that goal. Each strategic objective is further defined by a suite of performance goals that establish the level of performance to be achieved.¹¹ VA's OIT information resources management activities support IT development across VA, thereby supporting objectives in all VA strategic goals that have a technology component.

The Department's three APGs, shown in Figure 3, support improvements in near-term outcomes, customer service, and efficiencies. Additionally, the APGs advance progress toward longer-term, outcome-focused strategic goals and objectives in the agency's Strategic Plan. The VA APGs for FY 2015 focus on improving direct service delivery to Veterans and eligible beneficiaries by VA employees.

Agency Priority Goal 1 *Improve Veteran Access to VA Benefits and Services*

Improve client and stakeholder awareness of, and access to, VA benefits and health care services. By end of FY15, maximize the use of virtual service options to increase the number of claims received electronically.

Agency Priority Goal 2 *Eliminate the Disability Claims Backlog*

Improve accuracy and reduce the time it takes to complete disability benefit claims. Eliminate the disability claims backlog and process all claims within 125 days with 98% accuracy in FY15.

Agency Priority Goal 3 *Eliminate Veteran Homelessness*

In partnership with the Department of Housing and Urban Development (HUD), reduce the number of unsheltered homeless Veterans.

Figure 3 – VA Agency Priority Goals

The APGs are part of VA's Performance Management process—implemented quarterly as required by the Government Performance and Results Act (GPRA) Modernization Act—to enhance public transparency of performance data. The APGs are covered in more detail in the *VA Enterprise Roadmap*.

¹¹ *VA Strategic Plan FY 2014-2020*, March 6, 2014



1.2 OIT Mission, Vision, Strategic Goals, and Priorities

OIT provides information technology support across the Department for the sole purpose of ensuring VA's mission, vision, strategic goals and objectives, and APGs are met. In alignment with this purpose, Figure 4 shows OIT's mission and vision:^{12 13}

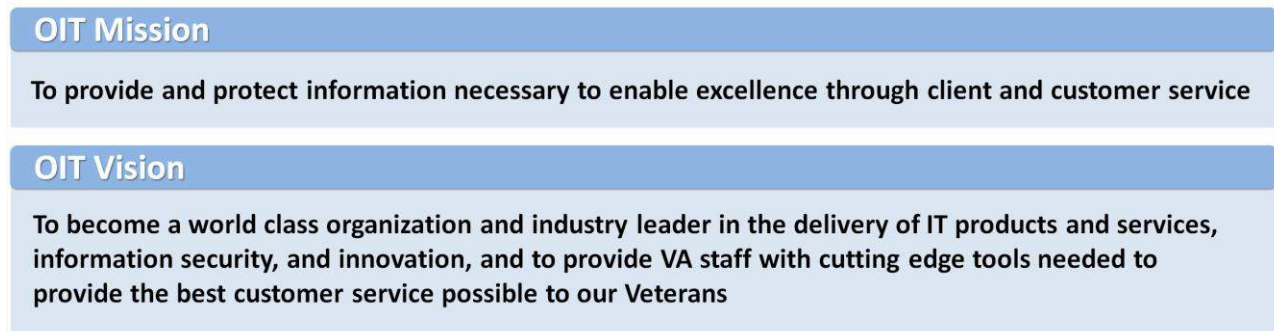


Figure 4 – OIT Mission and Vision

Technology and the resources required to support it underpin every aspect of the care, benefits, and services we deliver to Veterans. Information technology 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 health care, improved benefits processing, and provision of enhanced customer care and service to Veterans and their beneficiaries.

OIT Strategic Goals

In response to the *VA FY 2014-2020 Strategic Plan* and the APGs, OIT has developed goals and objectives that will support and enable the Administrations and staff offices, as shown in Figure 5, OIT Goals and Objectives.

¹² *Functional Organizational Manual Version 1.1*, September 2013

¹³ *VA IT Strategic Plan FY 2012 – 2015*, November 2012



Figure 5 – OIT Goals and Objectives



OIT objectives directly support numerous VA strategic goals in a “many-to-many” relationship, as shown in Figure 6, which illustrates the alignment between OIT objectives and VA strategic goals. To depict those relationships, the graphic shows that many of the OIT objectives span multiple VA goals. OIT objectives are aligned directly underneath those specific VA goals they support.

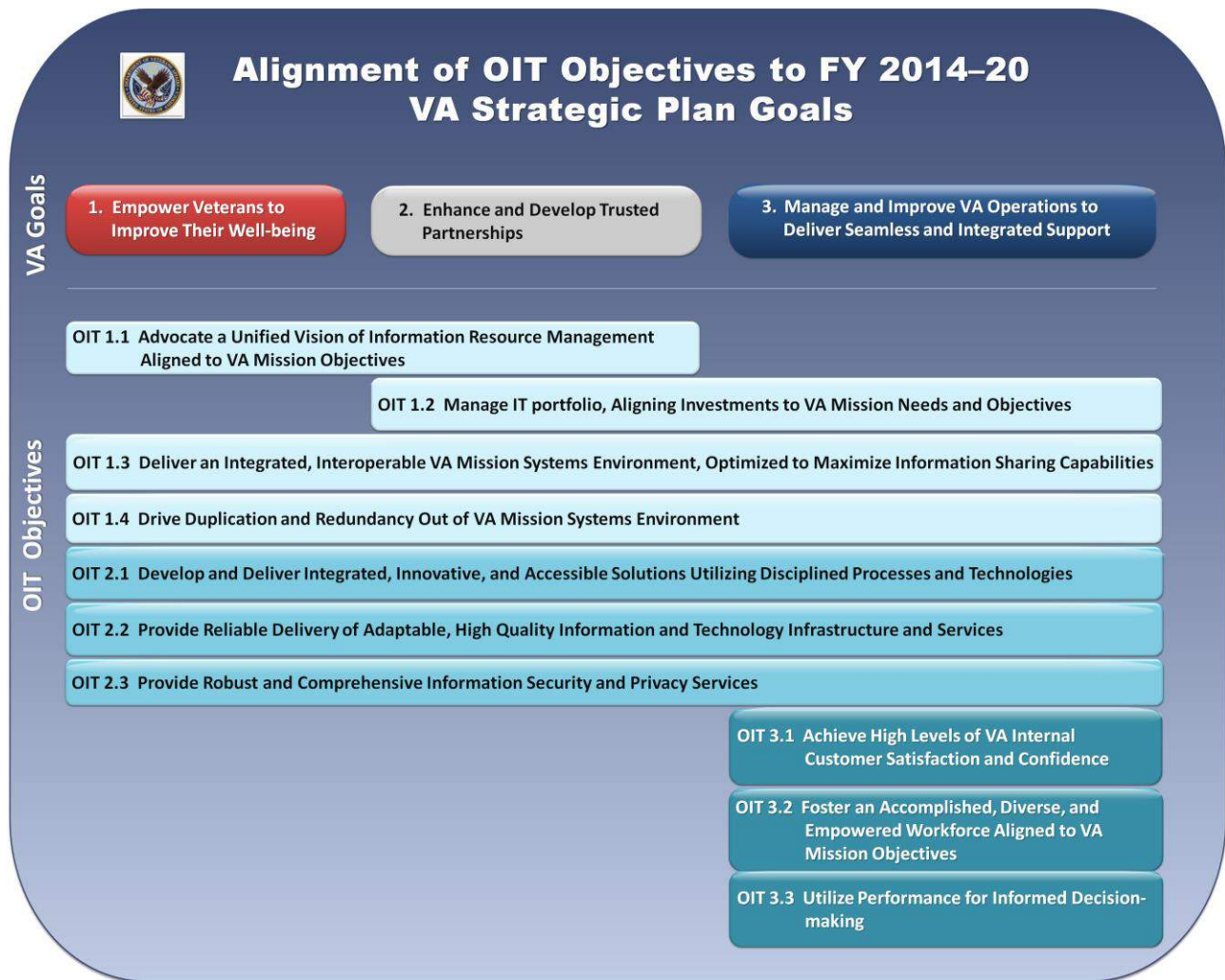


Figure 6 – Alignment of OIT Objectives to VA FY 2014-2020 Strategic Goals



CIO Strategic Priorities

To successfully provide the timely IT services and programs our Nation's Veterans deserve, the Assistant Secretary for Information and Technology (the Department's CIO) refocused the IT mission on 5 strategic priorities: customer service in every area of IT, next generation information security, transparent operational metrics, product delivery through system development processes, and fiscal management. These priorities mirror the Secretary's vision to transform VA to become a 21st century organization that is people-centric, results-driven, and forward thinking.

Customer Service

Customer service is about ensuring a high-level of committed and responsive IT support to VA's Administrations and staff offices. Keeping VA's IT systems secure and furnishing employees with access to high performing IT products is important in sustaining OIT's mission to provide and protect information necessary to enable excellence through client and customer service. For example, implementing capabilities for improving Veterans Relationship Management (VRM), one of the Secretary's major initiatives, will provide on-demand access to VA services and benefits through a multi-channel customer relationship management approach. VRM is designed to improve the speed, accuracy, and efficiency by which information is exchanged with Veterans. Optimizing IT systems affecting service delivery, supporting a robust analytic capability across VA, and building a qualified, professional IT workforce are other ways the CIO plans to improve customer service within OIT.

Next Generation Information Security

OIT is committed to creating a next generation information security plan to make VA one of the best in the Federal Government from an actual on-the-ground security posture. As part of this commitment, OIT has embarked on several projects to create a 21st century, world class security program that enhances information services to Veterans, improves compliance with legislation and regulations, and increases security awareness for the user community. With the Visibility to Desktop (V2D) tool, VA can, at any given time, from a central location at the enterprise level, verify deployment of security measures (antivirus, host-based intrusion prevention, endpoint encryption), current patch status of operating systems and applications, and security configuration status of over 300,000 assets in the VA network. This visibility will give OIT a comprehensive view of vulnerabilities in the VA network. The VA Medical Device Protection Program (MDPP) is another significant step in securing VA medical devices from cyber threats through isolation architecture. Medical devices can restrict the application of operating system patches and malware protection updates, which can create risk to the protection of patient sensitive data. OIT is committed to securing all VA medical devices through isolation architecture.

Transparent Operational Metrics

The focus in operational metrics is on availability and response times to our customers, considering metrics that OIT can derive benefits from, and moving forward to consolidate IT environments. OIT developed a standard set of enterprise-wide performance metrics for measuring the effectiveness of IT service delivery and is tracking these metrics to identify long-



term strategies through the Rigor and Performance Report and Monthly Performance Reviews. Metric examples include system availability, system response, and customer response. The creation and adherence of defined Service Level Agreements (SLAs), as well as the implementation of accurate, consistent, and frequent data collection, will improve performance to top standards.

Product Delivery

To proactively manage VA's IT projects and ensure IT program managers have access to the resources and tools they need, OIT established a formal process for project management. The 2009 published PMAS contributes to the delivery of functionality that meets IT business needs and improves VA's ability to provide benefits and services to our Nation's Veterans. Each of VA's major IT initiatives is held to critical program standards and consists of a series of project increments that are held to PMAS standards. The incremental approach ensures the customer, project team, and stakeholders working on a project are aligned by a single compelling measure—delivering functionality in cycles of 6 months or less. The benefits of PMAS include providing near-term visibility into troubled programs, better insight into scarce resources, frequent deliveries to customers to keep project functionality on track, and increased probability of successful programs.

Fiscal Management

VA has ranked all spending for all IT projects and services and now reasonably can determine how many should be successfully accomplished. To increase appropriate and timely spending requires tracking every IT budget dollar through several approaches to present a balanced view. The Project Management Accountability System (PMAS) allows for the recognition of insufficient resources and, therefore, stops failing IT projects in the beginning stages. The IT Dashboard shows the status of projects that comprise VA's IT development activities, providing greater transparency into cost, schedule, and overall performance of each IT project. The Budget Tracking Tool (BTT) is an integrated, enterprise-wide budget management and reporting system to support OI&T's current and future spending plans. A financial restructuring effort is in process to improve internal controls and IT spending across the board. These tools will help OI&T manage all IT assets and projects with full transparency and efficiency, valuing every dollar provided to advance IT for VA customers and staff.



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

Close collaboration exists between VA departmental strategic planning, Enterprise Architecture, and planning efforts within both OIT and the Administrations to ensure alignment among VA strategic goals, objectives, and APGs; OIT goals, objectives, activities, and priorities; and Administration-specific business segment requirements.

The VA OPP leads the VA Strategic Planning Process, which involves examining changes in environmental conditions, understanding the long-term implications of strategic goals, developing alternate strategies for addressing the changing environment, and determining and validating the strategic capabilities required to posture the Department for success in the future. The VA Strategic Planning Process, shown in Figure 7, results in the development of the *VA Strategic Plan* and establishes the Department's near-term strategic direction.



Figure 7 – VA Strategic Planning Process

The *VA Strategic Plan* serves as the benchmark against which all VA Administrations and staff offices build their goals and objectives as well as plan investment activities. Additionally, the plan establishes a direct line-of-sight traceability from VA goals, objectives, and strategies to IT investments. The *VA Strategic Plan* is used as the foundation of the VA IT Strategic Planning Process that is led by OIT, as shown in Figure 8.

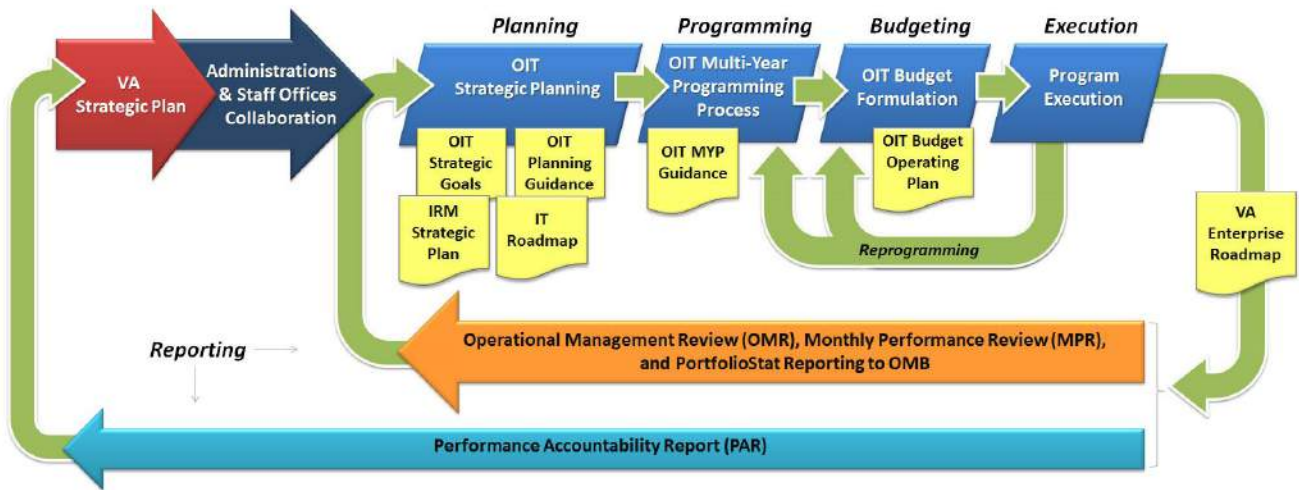


Figure 8 – OIT Strategic Planning, Programming, Budgeting, Execution and Reporting Process

The OIT PPBE process is an information resources management tool with four interrelated phases consistent with the Department’s IT objectives, policies, and strategies. Its purpose is to identify capability requirements (Planning), align them with resource requirements (Programming), translate resource requirements into budget proposals (Budgeting), and evaluate spending (Execution) to determine how well the desired IT capabilities are being achieved; all in alignment and integrated with the Department’s over-arching PPBE process.¹⁴ OIT’s adaptation of PPBE is in an early stage of maturation, with detailed processes and governance structures being developed. Below are descriptions of the intended process steps.

Planning – Establishes technology requirements and solutions to achieve VA strategic goals, objectives, and strategies while ensuring that information resources management decisions are integrated with organizational planning, budgeting, procurement, financial management, human resources, and program decisions.¹⁵

- **OIT Strategic Goals** – OIT senior leadership arrives at IT strategic goals by taking into account the future technical vision as described in the *IT Infrastructure Roadmap*, combined with VA strategic goals and objectives and the CIO priorities.
- **OIT Planning Guidance** – The *OIT FY 2015-2019 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.¹⁶ This guidance provides the analytic

¹⁴ *VA Information Technology Planning, Programming, Budgeting, and Execution Board (IT PPBEB) Draft Charter, Draft V.5.4, November 8, 2012, p. 1*

¹⁵ *VA Planning Guidance (FY) 2016-2020 Memorandum, September 27, 2013, pg.4*

¹⁶ *OIT FY 2015-2019 Planning Guidance, March 1, 2013*



framework for multi-year resource recommendations, ensuring that the requirements of VA's health care delivery, benefits delivery, and memorial services are fully vetted and integrated into the FY 2015-2019 Multi-Year Programming. 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, strategic goals and objectives, and APGs.

- **VA IRM Strategic Plan** – The *VA IRM Strategic Plan* describes how IT resource management activities support the accomplishment of VA's mission and ensure that information resources management decisions are integrated with organizational PPBE, human resources management, and program decisions. OIT planners weigh both business priorities expressed in individual VA Administrations' strategic plans and the needs for VA IT infrastructure evolution (as expressed in the *VA IT Infrastructure Roadmap*) in developing this *VA IRM Strategic Plan*.
- **IT Infrastructure Roadmap** – The *VA IT Infrastructure Roadmap* describes VA's IT vision—looking at specific emerging innovations and projecting their role and impact on future VA operations. This future (target) state view of VA's IT infrastructure environment is intended to guide enterprise-wide IT planning and decision-making. The *VA IT Infrastructure Roadmap* will play a key role in influencing VA's IT budget, technology investments, and strategic decisions necessary to transform and modernize VA's IT capabilities to ensure that VA can continue to successfully execute its mission in the future, and serve the nation's Veterans.¹⁷

Programming – Programming is the Department's process for allocating, balancing, and integrating resources among various programs according to VA priorities. For IT investments, programming identifies and allocates IT resources from an enterprise perspective that maximize integration of cross-functional capabilities to the programs that best support achieving VA strategic priorities. This phase includes identification and analysis of alternative strategies, and the application of technology and economic assessments.

- **OIT Multi-Year Programming (MYP) Guidance** – This is a highly collaborative process that engages stakeholders 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 MYP are numerous OIT Programming and Budget documents.

Budgeting – The outcomes of the MYP effort prioritize all proposed and ongoing IT investments; perform budget impact assessments for newly proposed investments; review annual budget

¹⁷ *Information Technology (IT) Roadmap Target State Vision of the VA Enterprise Technical Architecture (ETA)*, Draft Version 2.15, December 28, 2012



submissions; and review reprogramming of funding recommendations. Accordingly, OIT budgeting utilizes this information to develop VA's IT component of the President's Budget and operating plans and provides justification for the approved programs, projects, and technology solutions.

- **OIT Budget Operating Plan (BOP)** – Provides a detailed financial spend plan that identifies funding needs, plans, approvals, and changes at the lowest multi-factor level of program or project requirement, obligation, and financial category. The BOP and related processes and automated systems provide the structure, discipline, and tools for planning, approving, managing, analyzing, reporting on, and determining performance of the annual budget execution program. The BOP is baselined for performance measure tracking but is flexible, which allows OIT to respond to changing executive priorities and program requirements.

Execution – Involves developing and delivering the required technology solutions to support and establish the capabilities needed to achieve VA strategic goals, objectives, and strategies.

Reporting – Involves OIT performance reporting and program management reviews to ensure that execution is in accordance with the Department's established policies, guidance regarding program execution, and Administration requirements.

VA Performance Accountability Report (PAR) – Per the GPRA Modernization Act and OMB Circular A-11, VA is required to establish an annual performance plan, including performance goals, for each program in the budget submission and then report on the results. The VA PAR provides this annual reporting and presents accomplishments towards improving the timeliness, accessibility, and quality of health care and benefits service delivery.

- **Operational Management Review (OMR)** – The OMR oversight model is used to allow the DEPSECVA to provide focused oversight of the highest priority Department programs. Key elements of the OMR oversight model include review and approval of planning documents, reporting of performance against the approved plans, and routine performance meetings (OMRs) with the DEPSECVA and senior VA leaders.
- **VA Monthly Performance Review (MPR)** – The VA MPR is a briefing chaired by the VA Deputy Secretary. Performance presentations are based on operating plans of each VA Administration and staff office to describe the progress made in meeting established monthly and Fiscal Year To Date performance goals. The VA MPR is aligned with VA strategic goals and uses a Balanced Scorecard to assess performance. The VA MPR is designed to help VA leadership improve decision-making within the context of performance, budget, and workload results.
- **OIT Performance Review (PR)** – Performance review in OIT is a continuous process that occurs throughout the organization. The OIT PR is a series of performance reviews conducted within OIT by leadership to review progress toward achieving performance goals established by the CIO and Executive Leadership Team (ELT). The key purposes of the OIT PR are to report progress on achieving a goal or fixing a problem, to alert the ELT to monitor items that are trending negative, and to make informed decisions based on data.



Each OIT performance goal includes a risk assessment and one or more performance measures to reflect progress. Performance measures are also aligned with VA strategic goals and objectives.

- **PortfolioStat Reporting** – VA provides three outputs to OMB through the PortfolioStat reporting process: the *VA IRM Strategic Plan* (annually), the *VA Enterprise Roadmap* (annually), and Integrated Data Collection data from program execution (quarterly).
 - The *VA Enterprise Roadmap* provides insight into the state of VA’s transformation efforts through program execution. It describes VA’s EA program and provides details of VA’s most critical segments, current state, and future visions of approaches, strategies, and initiatives in place to facilitate transition.
 - VA Integrated Data Collection is a channel to report progress in meeting IT strategic goals, objectives and metrics, as well as cost savings and avoidances resulting from IT management actions. Integrated Data Collection draws on information previously reported under PortfolioStat, the Federal Data Center Consolidation Initiative, the Federal Digital Government Strategy, quarterly Federal Information Security Management Act metrics, the Federal IT Dashboard, and selected human resource, financial management, and procurement information requested by OMB.¹⁸

¹⁸ OMB Memo M-13-09, *Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management*, March 27, 2013



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

The CIO authorities as defined in statute and policy (e.g., U.S.C. § 38, 40, and 44 and OMB Memorandum M-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 has 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 the 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 the Office of Information and Technology. 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 OIT's strategic goals and the CIO's priorities as shown in Section 1.2.

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 VA of IT-related initiatives and legislation; and sharing lessons learned. To meet its responsibilities and challenges, OIT is organized as shown in Figure 9.

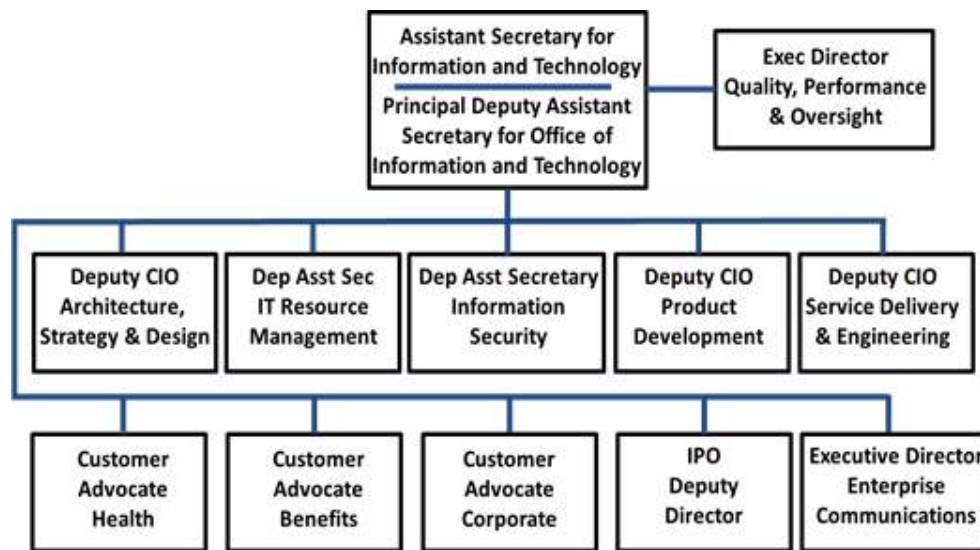


Figure 9 – Office of Information and Technology (OIT) Organization Structure

According to the *VA Functional Organizational Manual (FOM)*, Version 1.1, dated October 2013, the following OIT organization descriptions are provided.¹⁹

Architecture, Strategy, and Design (ASD) provides strategic planning and EA alignment and program development support for the VA IT environment. It also 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 Enterprise Architect establishes and manages the EA and IT strategy elements for VA as required in the Clinger-Cohen Act, in accordance with VA Directive 6051.²⁰ ASD creates standards for implementation of IT solutions that best serve Veterans and VA employees through the integration of technical, business, and data architecture, IT strategy, systems design, and knowledge management, while exercising proper stewardship of resources and maintaining transparent operations.

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.

¹⁹ *VA Functional Organizational Manual* –Version 1.1, October, 2013

²⁰ VA Directive 6051, *VA Enterprise Architecture (EA)*, July 12, 2002



IT Resource Management (ITRM) advises the AS/IT and other senior OIT officials on OIT resource requirements. The office is responsible for the management of all IT resources, direction of financial and IT asset management, and the policies and strategic planning activities for OIT acquisitions. With primary responsibility for linking the budgeting process with IT programs, ITRM is responsible for directing fiscal activities related to linking the budget process to all established IT operations and enterprise-wide management initiatives. Offices within the organization include IT Budget and Finance; IT Acquisition Strategy and Space/Facilities Management; IT Workforce Development; and IT Business Relationship Management.²¹

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 health care, 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.

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 PMAS Business Office.

PD has execution and oversight responsibility for all enterprise application development and is the chief advisor to the AS/IT for all enterprise application development activities. Development consists of planning, developing (or acquiring), and testing applications that meet business requirements. It provides day-to-day direction and overall solutions developed by OIT for VA business units. PD provides IT program oversight (beyond CIO authorities) to centralize and oversee all program development. PD ensures visibility across all IT development activities to

²¹ *Welcome to ITRM Manual*, ITRM Functional Statement, June 2011



increase consolidation of application development, and promote the migration to services orientation, and support the standardization and reuse of services and applications.

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 on behalf of the Assistant Secretary. It oversees and manages VA regional data centers, the IT network, and telecommunications; monitors production for all information systems and production services; delivers operations services (including deployment, maintenance, monitoring, and support) to all VA geographic locations; and conducts all private branch exchange management and maintenance. 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, administrative field services, 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) work with the Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), National Cemeteries Administration (NCA) and VA's staff offices at senior levels to ensure that issues of mutual concern are resolved. There are three CAs focused on health care 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 issues resulting from the PMAS and work across VA to identify and facilitate the resolution of any IT issues relating to VA mission support. The advocates act as an Ombudsman between OIT and its customers, providing a single access point for customers to communicate with senior IT leadership.

Interagency Program Office (IPO) – Integrated Electronic Health Record (iEHR), the VA/Department of Defense (DoD) IPO, was established by the National Defense Authorization Act for FY 2008. This body serves as the single point of oversight and accountability for the Department in the development and implementation of the iEHR system, capabilities, and initiatives with the goal of full interoperability between DoD and VA.

Office of Enterprise Communications (OEC) has the responsibility for all voice, data, and video systems, as well as network transport. Within this oversight, OEC monitors and manages the network down to the "facility edge," and is responsible for the budget, capacity planning, and design (in conjunction with Enterprise Systems Engineering) of all communications systems and infrastructure enterprise-wide.



Quality, Performance, and Oversight (QPO) serves as advisor to the AS/IT on a wide range of complex and sensitive issues, which cross organizational boundaries within the Department, and interfaces with external agencies, such as OMB, Government Accountability Office (GAO), Office of Inspector General (OIG), and Congress. QPO consists of the Office of Enterprise Risk Management, Office of Policy, Performance and Oversight, Office of Project Coordination Service, Office of Executive Correspondence, and Systems Quality Assurance Service.

QPO leads OIT's performance management, process improvement, and oversight efforts. The Office 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. It conducts analysis and evaluation of a variety of IT programs, processes, functions and facilities, and provides recommendations to the AS/IT.

Within QPO, the Office of Enterprise Risk Management (ERM) provides 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. ERM acts as an independent enterprise risk appraisal function by determining if OIT risk management, controls, and governance processes, as designed and represented by OIT management, are adequate and functioning as anticipated.



3 Governance and Management Processes

Governance is the vehicle that enables VA to control and manage decision making. The link between VA Governance and IT Governance is crucial to ensure VA's business strategy and the Administrations' programs set the direction for IT strategy and development. Benefits include cost savings, increased efficiency and efficacy, faster and easier access to information, improved service, and greater reliability.

VA has centralized and consolidated authority for all IT activities under the AS/IT (VA CIO). The AS/IT is responsible for both the formulation of the IT budget and management of the IT portfolio, as well as direct management control of all IT programs.

The VA is establishing disciplined, integrated governance for the VA PPBE process. This document will reflect the PPBE governance evolution as it matures. The following sections provide a description of governance boards and management processes currently in place.

3.1 VA Executive Governance

The AS/IT (VA CIO) engages the Department's senior leadership to chart the overall course of the Department's capabilities as well as establish Department-wide priorities and alignment of IT activities to support them. 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 Chairman of the Board of Veterans' Appeals. The VA CIO, as the AS/IT, is a member of the VAEB.

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 Chairman of the Board of Veterans' Appeals. The VA CIO, as the AS/IT, is a member of the SMC.



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 Governance, Investment, and Portfolio Management (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 strategic and business objectives of the Department in an efficient and effective manner. The two boards described below have been established to provide executive oversight to 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 IT Planning, Programming, Budget and Execution Board (IT PPBEB). In addition to approving the IT MYP, the ITLB makes recommendations to the SRG regarding strategy, planning, programming, budgeting, and execution of IT services. The board also addresses budget formulation and execution issues that cannot be addressed by the IT PPBEB. The ITLB is chaired by the AS/IT (VA CIO) and includes executive membership from each VA Administration and major staff office.

3.2.2 IT Planning, Programming, Budget and Execution Board (IT PPBEB)²²

The IT PPBEB is an OIT-led IT governance board with Department-wide participation that ensures VA optimizes standardization, interoperability, security, reliability, and flexibility of technology infrastructure across the enterprise, as well as adherence to information protection standards and initiatives. The IT PPBEB monitors alignment of IT programs and systems for consistency with the Department's Strategic Plan, Administration and staff office Line of Business priorities, *VA IRM Strategic Plan*, and Enterprise Architecture. The IT PPBEB replaces the functions previously provided by the Programming Long Term Issues Board (PLTIB) and the Budgeting and Near Term Investment Board (BNTIB).

The IT PPBEB is designed to play a critical role in VA's IT governance structure in selecting, reviewing, and assessing IT capital investments. The IT PPBEB will consider all IT resource issues

²² *VA Information Technology Planning, Programming, Budgeting, and Execution Board (IT PPBEB) Draft Charter, Draft V.5.4, November 8, 2012*



and will forward appropriate recommendations to the ITLB for decision-making. The IT PPBEB will make appropriate decisions regarding budget formulation and execution matters. The IT PPBEB is chaired by the Deputy Assistant Secretary for ITRM. The members include senior executives from each VA Administration and major staff offices. The action, decisions, and outputs of the IT PPBEB feed directly into the Department-level PPBE process. This helps to ensure that the Department fulfills its mission as effectively and efficiently as possible while providing analytical rigor to justify its resources.

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

All IT system development within VA is done in accordance with VA Directive 6071, PMAS. To ensure that development activities deliver expected capabilities within planned time and budget constraints, the CIO implemented the PMAS.²³ PMAS 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. 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.

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 a CIO Congressional Certification Letter.²⁴ 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 state is entered only with the successful completion of the previous state's activities, which are 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.

As defined by VA 6071, Milestone Reviews are mandatory decision points, which are conducted by the Office of Responsibility (OOR). Milestone approval is required for a project to enter the Planning, Active, and Closed PMAS states. Milestone 1 Reviews are required prior to each subsequent delivery increment. Milestone 2 Reviews are required prior to all deployment increments. The frequency of each project's Milestone Review is defined by VA 6071 and the

²³ *PMAS Directive*, February 20, 2013

²⁴ *PMAS Guide 4.0*, November 17, 2012



PMAS Guide. Each Milestone Review requires the completion of a defined set of project activities and artifacts. Milestone Reviews function as stage gate reviews that verify whether a project is ready to begin work in the next state or increment. They are chaired by a Deputy Assistant Secretary/Deputy CIO (DAS/DCIO) or his/her Senior Executive Service (SES) representative from the appropriate OOR, and are convened as required. Senior OIT leaders, including the OIT Executive Leadership Team (Deputy CIOs and Deputy Assistant Secretaries), and all applicable OOR leaders within OIT are present at each Milestone Review and are actively engaged in approving a project's entry into the next PMAS state.

3.4 Enterprise Risk Management (ERM)

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 is determined, they are presented to the AS/IT. OIT ERM Risk Assessment and Mitigation (RAM) teams are available to assist the AS/IT and each OIT organization by performing root cause analyses, compliance assessments, recommending risk response and mitigation strategies, and performing post-mitigation assessments.

3.5 IT Process Asset Library

The IT Process Asset Library is a one-stop shop providing critical links to the formally approved standard processes, artifacts, standards, tools, and templates used to assist the OIT workforce in performing their daily work. The Asset Library is accessed and managed using an innovative process and procedure repository called ProPath, which is integral to VA IT governance, investment management, and life cycle management approaches. ProPath provides an "at-a-glance" perspective of nearly every process in the IT life cycle, associated roles and responsibilities, and the required templates, tools, and standards.

Process Management, within the OIT ASD organization, is responsible for the development, implementation, operations, and maintenance of the IT Process Asset Library. ASD works with the OIT workforce to build and maintain ProPath to document the ever changing OIT business architecture. Working with the OIT workforce and guided by the Executive Leadership Team, Technical Working Groups and Process Leaders identify continuous process improvement opportunities. Updated processes, standards, roles, and template changes are fielded in ProPath releases on a quarterly basis, at minimum.



ProPath was created to enhance and encourage the use of standard and repeatable processes across OIT. ProPath's use has resulted in improved workforce productivity; lower costs by reducing rework; and less variance in product and service quality. By using the processes and templates, and understanding the roles, responsibilities, and durations of activities, the workforce can perform their duties confident that their actions are compliant with policy, standards, and regulations, as well as consistent with best practices. Since ProPath enables visibility into existing processes, standards, and tools used by the OIT workforce, it is a critical tool in helping leadership and the workforce identify and capitalize on opportunities for cost containment and reduction; make process changes required to react to emerging technologies and situations; and improve organizational performance and informed decision making.

3.6 Evolving VA Corporate Enterprise Processes (CXXC, CXXD)

VA corporate enterprise processes are currently undergoing transformation. VA is defining two new enterprise processes: PPBE and Acquisition Program Management Framework (APMF). Once implemented, these enterprise processes will greatly enhance the Department's ability to do three things: identify the capabilities needed to support VA strategic goals; identify and align business, technical, and financial requirements for those capabilities; and execute appropriate acquisition strategies to operationalize those capabilities. VA is in the early stages of defining the relationships among these enterprise processes and understanding how they can be optimally linked.

3.6.1 Planning, Programming, Budgeting, and Execution (PPBE)²⁵

PPBE will enable the fulfillment of the Department's strategic priorities via a fully informed and repeatable resource allocation process as depicted in Figure 10. The Planning function identifies the Department's strategic priorities and derives the strategic capabilities and requirements needed to achieve those priorities. The Programming function applies resources to programs that will ensure delivery of the capabilities identified in Planning. The Budgeting function builds the budget artifacts and justifications for the program decisions as well as seeks the funding required for execution. The Execution function enacts the Department's budget via business and operational plans and measures how well the Department is performing its mission.

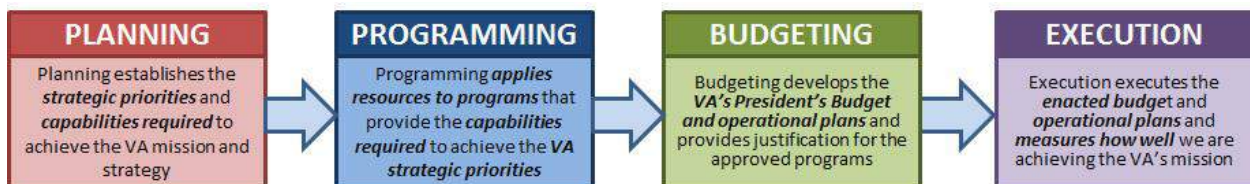


Figure 10: Planning, Programming, Budgeting, and Execution (PPBE) Process

²⁵ VA Programming Guidance Fiscal Year 2016-2020 PPBE Cycle, September 16, 2013



This resources allocation process requires alignment between the four functions to ensure that strategic decisions made during each function inform subsequent phases within the PPBE. It is an integrated, multi-year resource allocation process that provides a structured and data-driven approach for VA to assess its needs, allocate resources, and produce a budget that delivers high quality and timely benefits and services to Veterans. One of the outcomes from a successfully implemented PPBE will be better investment decisions, to include IT portfolio selection and IT portfolio management.

3.6.2 Acquisition Program Management Framework (APMF)

A critical element to establishing a fully integrated set of enterprise core processes will include the implementation of the APMF, which was approved by VA’s SMC on May 1, 2013. The APMF will provide overall guidance and structure for acquisition program management to support the orderly acquisition of needed capabilities across VA. The APMF will improve VA acquisition capabilities by providing more disciplined approaches to all aspects of program management, cost estimating, requirements management, and systems engineering. When implemented, the APMF will consist of a tailorable, five-phase process for all acquisition programs, beginning with verification of approved and funded capability shortfalls that require a physical solution and extending to solution retirement as depicted in Figure 11.²⁶

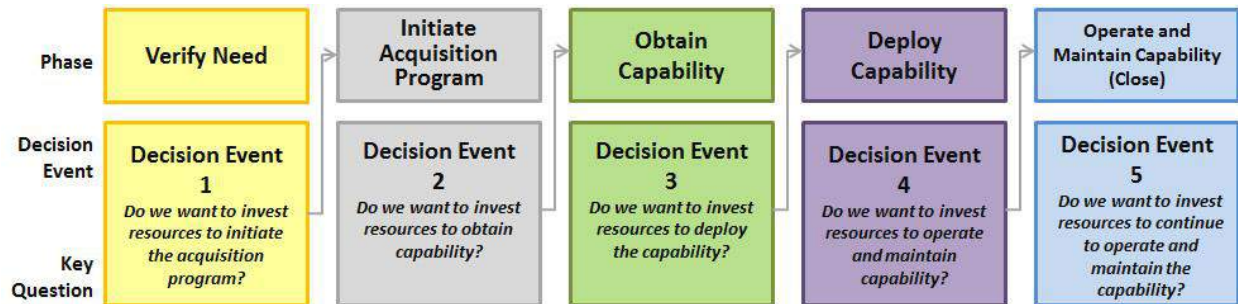


Figure 11: Acquisition Program Management Framework (APMF)

The APMF implementation is being guided by the Malcolm Baldrige National Quality Award criteria. Implementation of the APMF is being conducted at VA on a limited scale through pilots beginning 3Q FY14 and roll out of increments to include Initial Operational Capability (IOC) by 3Q FY15 and Full Operational Capability (FOC) by 4Q FY15.²⁷ This plan demonstrates successful

²⁶ Program Management Summit, Performance Excellence, The Baldrige Criteria, and The Program/Project Manager, January 29, 2014

²⁷ Program Management Summit, Acquisition Program Management Framework (APMF) Implementation, January 29, 2014



application of GAO’s recommendation to implement a governed acquisition program life cycle structure.²⁸

The APMF is equally compatible with IT, construction, and services-based acquisition, and flexible enough to accommodate PMAS and Agile project frameworks and methodologies. VA is in the midst of programming a 5-year capabilities requirement proposal to articulate the requirements and resources VA will need to establish the APMF Department-wide and budget them within the FY16-20 timeframe.²⁹

3.6.3 End-to-End Requirements Management (E2ERM)

E2ERM is a methodology for the generation of appropriate requirements throughout the PPBE to inform resource allocation decisions and execution. As depicted in Figure 12, this methodology calls for line of sight linkages from the Strategic and Business capability requirements identified during the Planning and Programming functions of PPBE to the Acquisition, Project, System, and Contract Requirements developed during the Budgeting and Execution functions in support of PPBE.

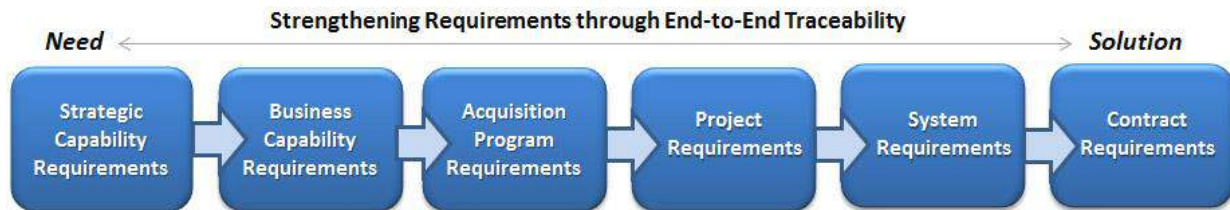


Figure 12: End-to-End Requirements Management (E2ERM)

²⁸ *Acquisition Program Management Framework (APMF) Update*, submitted to the Strategic Management Council, May 1, 2013

²⁹ *Department of Veterans Affairs Programming Guidance Fiscal Year 2016-2020, PPBE Cycle*, October 11, 2013, pg.24



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

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.

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 mostly been that information about any individual Veteran is fragmented and incomplete. This paradigm no longer works in today’s environment.

VA has been embracing this challenge and adopting a “Veteran-centric” approach to deliver health care and economic benefits to Veterans through business processes that start with the needs of the Veteran—not the convenience of VA. This approach involves establishing a relationship with every Veteran the day they enter military service and evolves throughout their lifetime. To be truly “Veteran-centric,” VA’s goal is not only to 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. The accompanying *VA Enterprise Roadmap* lays out a full range of activities in greater detail, which VA has done or is in the process of completing. The two services discussed below—MyHealtheVet and eBenefits—represent some of the key, “Veteran-centric” transformational efforts in place at VA.

MyHealtheVet

MyHealtheVet is a web-based application where Veterans, family, and clinicians may come together to optimize Veterans’ health care. This web technology combines essential health record information enhanced by online health resources to enable and encourage patient/clinician collaboration. The implications of MyHealtheVet 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 their health care providers, inside and outside VA. This has the potential to dramatically improve the quality of care available to our nation’s Veterans by providing a 360 degree view of Veteran’s medical history to all of their



providers. Through Veteran empowerment, Veterans can better understand and manage their health and better assess the potential gain and risk of proposed medical interventions. Key portions of a Veteran's DoD Military Service Information are now available in MyHealtheVet. This new feature is available to military retirees and/or Veterans discharged after 1979.

Also available for use on MyHealtheVet is VA's Blue Button feature that enables Veterans to download, view, store, print, and transfer information from their VA Personal Health Record as Portable Document Format (PDF), text files, or Blue Button output files. User can also track when Blue Button was used to download their health information via the MyHealtheVet Account History Activity log. Veterans who have been authenticated have the ability to download and view VA Wellness Reminders and VA Appointments. Additionally, Blue Button allows Veterans to download their Military Occupation Specialty data. In 2013, the VA Continuity of Care Document (VA CCD) tool was added, which contains a summary of the Veteran's essential health and medical care information in Extensible Markup Language (XML) and PDF file formats—recognized standards that support the exchange of health care information. For the first time, Blue Button marks the availability of a truly portable electronic health record that can be stored, shared, and reused, in whole or in part, by any Veteran with the people and tools they trust.

eBenefits

The eBenefits Portal is a one-stop shop that provides wounded, injured, and ill Servicemembers, Veterans, their families, and care providers with a single sign on (SSO), central access point to online benefits and related services. The eBenefits Portal provides:

- A tailored, self-service portal that meets the unique needs of the Servicemember, Veteran, or family member, with information and tools relevant to their specific circumstances and physical limitations
- A single sign on Web site that will serve as a central hub for users to gain access to related, supporting VA and the DoD benefits and information services
- A safe and secure manner by which users can access their personal information
- A user-friendly means of connecting to relevant VA and DoD information that is easy to navigate and understand
- A decision support capability that will provide users with eligibility pre-determination assistance and support based on the user's unique information
- Simple and direct communications and messaging channels through which users may ask questions or gain relevant information

Veterans now have improved access to benefits information from multiple channels—on the phone, online, and through our shared DoD/VA portal called eBenefits which currently has 3.6 million users. In FY 2013, the number of eBenefits users increased by 51% over the number of users in FY 2012.

Veteran Online Application Direct Connect (VDC) leverages eBenefits as a means for users to prepare and submit electronic claims. VDC's form wizard makes it easier for Veterans to answer a series of logical interview questions to request benefits, which will improve the customer



experience and satisfaction, versus completing a complex form. Claims are maintained in an electronic form, which allows them to be processed anytime and anywhere to reduce or eliminate paper storage costs.

Additionally, VA is relying on Veterans Service Organizations (VSOs) to continue to perform their vital advocacy and assistance role within VA's transformed benefits delivery model. The Stakeholder Enterprise Portal (SEP) is a secure, Web-based entry point that complements eBenefits and gives VSOs and other authorized advocates access to assist Veterans with electronic claim submissions. Using the portal, registered users can check the status of claims, review payment history, and upload documentation on behalf of the Veterans they represent—all within a digital environment. When filing a claim online in eBenefits, a Veteran can request the assistance of a VSO by choosing from a list of accredited representatives in VA's database. When logging into SEP, the chosen VSO representative is alerted to the Veteran's request, and upon acceptance, is given power-of-attorney authorization to access the Veteran's claim and assist with preparation. Once the VSO representative believes the claim is ready for submission they send notification back to the Veteran via eBenefits and then the Veteran submits the claim to VA.

4.1 Open Government

VA strongly supports the Federal Government movement to make government information more transparent, understandable, and accessible under the overall heading of Open Government. The Department has instituted its own Open Government initiative to address and implement OMB-introduced public initiatives. VA's efforts are designed to raise awareness of VA's mission and to facilitate the understanding of VA data and the impact of that data on the Veteran. Summaries of selected VA Open Government initiatives and their current status are presented below and in more detail in the *VA Enterprise Roadmap*.

4.1.1 The Open Data Initiative

Key to VA's Open Government activities is its Open Data initiative. The initiative is intended to make information easier for the public to find and to facilitate its reuse by developers, non-profits, and other third parties. The initiative also seeks to improve data collection and management processes within the Department. VA regularly offers VA information and datasets for public use on the Internet at www.va.gov/data, where it currently posts more than 470 datasets.



Opening and releasing non-sensitive data in well-structured, machine-readable formats allows innovations both in and out of government to develop new tools, integrations, and insights to improve the lives of Veterans in meaningful ways. For example, VA's GI Bill Comparison Tool is an open-source application powered entirely by open VA and Department of Education data that allows Veterans and their dependents to compare GI Bill education benefits against collected data with just a couple of clicks. Other school comparison sites can use our GI Bill data to improve their services. A sampling of currently available VA data sets includes:

- **Patient Satisfaction Surveys:** These survey results offer a snapshot of the quality of care provided at VA health care facilities
- **Veterans Benefits and Compensation:** This dataset provides a count of the number of Veterans receiving disability compensation or pension payments from the Department of Veterans Affairs
- **Geographic Distribution of VA Expenditures:** This report shows estimated VA expenditures for major programmatic areas by geographic area (state, county, and congressional district)
- **Veterans' Gravesite Locations:** This includes more than 50 datasets for Veterans' gravesite locations in the 50 states and U.S. territories, which coincided with the release of an Application Programming Interface (API) (the Nationwide Gravesite Locations API) on VA's developer hub³⁰

VA is committed to meeting data transparency requirements and releases new data on at least a quarterly basis. VA is committed to providing Veterans and the public with high priority data that is clear, concise, easy to use, and fully compliant with the requirements of OMB M-13-13 to treat, collect, and store information as an asset.

4.1.2 Federal Digital Government Strategy Initiative

In planning Veteran-centric services, VA is leveraging the Federal Digital Government Strategy (FDGS)³¹ released May 23, 2012. The FDGS provides federal agencies with guidelines for using modern tools and technology to build a 21st century platform to better serve the American people. VA implemented digital capabilities according to the FDGS Milestones in order to deliver better digital services to Veterans, their families, and stakeholders as well as the VA workforce. The FDGS stresses a "Customer-Centric" approach to allow customers to help shape, share, and consume information whenever and however they want. This approach influences how data is created, managed, and presented through websites, mobile applications, raw data sets, and other modes of delivery.

³⁰ *Digital Government Strategy Report for the Department of Veteran Affairs*, May 5, 2013

³¹ Office of Management and Budget, *Digital Government: Building a 21st Century Platform to Better Serve the American People*, May 23, 2012



Key activities supporting the FDGS directive include:

- Installation of Digital Analytics Program tool to provide web performance metrics
- Use of the program *Foresee* to collect customer satisfaction metrics
- Use of social media (*Facebook and Twitter*) to inform Veterans and their beneficiaries
- Provisioning of the Veterans' gravesites API for access by mobile application developers
- Provided a prioritized list of mobile applications including Post Traumatic Stress Disorder (PTSD) Coach and Clinic in Hand Mobile Prescription Medication Refill

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 health care, 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 Servicemembers.

Several dozen mobile applications have been scheduled for development. As an example, listed below (Figure 13) are the applications in various stages of production for The Family Caregiver Program (formerly Center for Integrated Healthcare), which provides a suite of mobile applications aimed at patient care. Patients will use these applications to provide real-time data and information that offers a more complete and accurate snapshot of their needs, issues, priorities, activities, and health outcomes.



Mobile Application Name	Type of Patient Generated Data																	
	Appt Request Info	Assessment Results	PTSD Tool Use Results	Pain Mgt Goals	Calendar Events	Notifications	Device Registration	Communications	Daily Event	Diet	Documents	Exercise	Mood	Vitals	Advocate Request Form	RX Refill Request	Health Inventory Goals	Application User Feedback
Appointment Request (VAAR)	✓																	
Scheduling (VAAC)	✓																	
Health Assessment (CiH)		✓																
Care4Caregiver (CiH)		✓																
VA PTSD Coach (CiH)		✓	✓															
VA Pain Coach		✓		✓														
Notifications and Reminders (CiH)					✓	✓	✓											
Journal (CiH)								✓	✓	✓	✓	✓	✓	✓				
Health Advocate (CiH)															✓			
RX Refill (CiH)																✓		
MyStory																		✓
LaunchPad																		✓

Figure 13 – Sample from the Family Caregiver Program³²

As part of the Patient Generated Data (PGD) standardization effort that will impact programs such as Family Caregiver, VA OIT is actively engaged with the IPO iEHR Data Management Services team to document an end-to-end Data Federation solution that enables access to DoD and VA data.

The PGD implementations require:

- Ready capture of data remotely and at the point of care
- Data standardized and utilized across platforms
- Data sharing consistent with patient views and clinical needs
- Data identified as patient entered
- Optimized clinical workflow—balance value and burden
- Ready review of information and integration into clinical documentation

VA mobile platforms are designed to the highest mobile security and privacy standards available. VA is actively engaged in discussions on mobile privacy and security and incorporates all new federal security requirements developed by the Department of Homeland Security (DHS), DoD, and the National Institute of Standards and Technology (NIST) for mobile and wireless services

³² OIA_PG D project database, dated July 2013



into its enterprise policies and procedures. The Mobile Application Reference Architecture (MARA) being developed by VA OIT answers the following question:

If I were to build a VA-wide mobile application, what architectural layers, design patterns, standards, and tools do I need to comply to and/or consider?

VA's MARA consists of:

- Architectural layers of a mobile application
- Knowing the key scenarios where mobile applications would be used
- Understanding the design considerations for mobile applications
- Design constraints and challenges of building mobile applications
- Identification of specific scenarios for mobile applications, such as deployment, power usage, and synchronization
- Knowing key patterns and technology considerations for designing mobile applications

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. The following sections discuss a few of the key VA information sharing initiatives that support these activities.

4.3.1 Integrated Electronic Health Record (iEHR)³³

iEHR was established as a joint effort between VA and DoD to develop a concurrent method by which active and retired Servicemembers can access their health records. Specifically, VA and DoD were called upon “...to define and build a seamless system of integration so that when a member of the Armed Forces separates from the military, he or she will no longer have to walk paperwork from a DoD duty station to a local VA health center. Their electronic records will transition along with them and remain with them forever.”

In accordance with Section 713 of the FY 2014 National Defense Authorization Act (Public Law No: 113-66), the Secretary of Veterans Affairs and the Secretary of Defense are jointly collaborating to ensure that the electronic health record systems of the Departments are interoperable with an

³³ *Vista Evolution Program Plan, Version 1.20, October 24, 2013*



integrated display of data, or single electronic health record that complies with the national standards and architectural requirements identified by the IPO), which was launched in October 2011. Additionally, the goal of the Departments is to deploy modernized electronic health record software supporting clinicians no later than December 31, 2016.³⁴

However, in recognition of the increasing costs and risks emerging from the current implementation path, the Secretaries of VA and DoD announced on February 5, 2013 that the departments would accelerate the delivery of iEHR through focus on near-term interoperability goals. Additionally, the Secretary of VA announced that VA would achieve the 2014 IOC milestone by deploying an iEHR Core based on Veterans Health Information Systems and Technology Architecture (VistA), which is the current VA EHR system. Subsequently, the Secretary of Defense announced the decision to move forward with a competitive acquisition to determine the iEHR Core product with the intent of replacing their current EHR.

As a result, VA is now programmatically responsible for managing and delivering enhancements to VistA under the VistA Evolution Program while DoD is programmatically responsible for managing and delivering its EHR modernization program named DoD Healthcare Management System Modernization. The IPO is programmatically responsible for managing and delivering the seamless sharing of interoperable health data between the departments.

4.3.2 Identity and Access Management (IAM)

IAM provides VA with a single comprehensive longitudinal view of a Veteran or beneficiary electronic record across VA and DoD. IAM enables VA to rapidly search, identify, authenticate, and authorize who is accessing its information systems. IAM provides a shared enterprise infrastructure and enterprise services that can be consumed by internal and external VA user populations. IAM services enable VA “to create and maintain information systems that deliver more convenience, appropriate security, and privacy protection, with less effort and at a lower cost.”³⁵ This effort cuts across all VA programs, Lines of Business, and multiple initiatives including but not limited to: VRM, Human Capital Investment Plan (HCIP), Veteran Benefits Management System (VBMS), G.I. Bill, and Enhance the Veterans Experience and Access to Healthcare (EVEAH).

³⁴ FY 2014 National Defense Authorization Act (Public Law No: 113-66), SEC. 713. *Electronic Health Records of the Department of Defense and the Department of Veterans Affairs*

³⁵ *Report to Congress on Implementation of The E-Government Act of 2002* (FY 2009)



4.3.3 Customer Data Integration (CDI)

CDI is a new initiative designed to harmonize and sequence the exchange and use of digital information within the VA computing environment and between VA and its mission partners in the delivery of benefits to Veterans. Today, the ability of VA to fully integrate capabilities and services provided to Veterans is hindered by a legacy environment in which the same or similar information about Veterans is gathered and stored in multiple places—thus, discovery or recognition of authoritative sources of information is often impossible. While this redundancy and lack of data integration is often manifest as multiple overlapping databases, the root cause is typically business process-centric. Recognizing this, CDI efforts are focusing on the development of an enterprise-wide foundation—policies, governance, processes, and services—to manage customer data as a Department asset.³⁶

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 as the mechanism to leverage leadership across VA to build out the Department’s existing process and data architecture. The EA team is working with the CDI’s Business Integrator to build an Enterprise Logical Data Model for VA to enhance and support data standardization, recognition of data redundancy, and potential institution of single authoritative data sources, particularly in the area of “common customer data.” CDI represents a huge opportunity to engage every organization within VA in both the development and use of EA while simultaneously addressing a critical need of the Department.

³⁶ Customer data represents the first instance of common data. Other classes of common data will be developed as the architecture is constructed.



4.3.4 Architecture

VA's EA was established as the "explicit description and documentation of the current and desired relationships among program/business and management processes and information technology."³⁷ VA is developing and managing the OneVA EA using a federated approach. This approach necessitates a partnership across the enterprise between the VA Chief Enterprise Architect and VA Administration architects, functional business process owners, OIT leaders, and other Department EA stakeholders.

VA continues to evolve and improve the OneVA EA to make it useful for decisions that support the VA mission. The EA effectiveness is evidenced by:

1. Commitment of Administrations' business architecture leadership to collaboratively build the OneVA EA
2. Use of OneVA EA artifacts to inform IT multi-year planning guidance and IT budget development
3. Publication of EA "Compliance Criteria" which are used to assess how well projected designs align with the rules and standards in the Enterprise Technical Architecture (ETA)

As a result, the OneVA EA is increasingly embedded in strategic planning and transformation leadership processes across the Department. More information on the OneVA EA program is provided in the *VA Enterprise Roadmap*.

³⁷ Department of Veterans Affairs, VA Directive 6051, *Enterprise Architecture*, July 21, 2002



5 IT Infrastructure Optimization

The VA enterprise IT infrastructure provides the backbone upon which OIT delivers the necessary technology and expertise to achieve VA’s mission, goals, and objectives. Figure 14 depicts OIT’s technology framework, which provides a structure to guide the evolution of VA’s IT infrastructure.

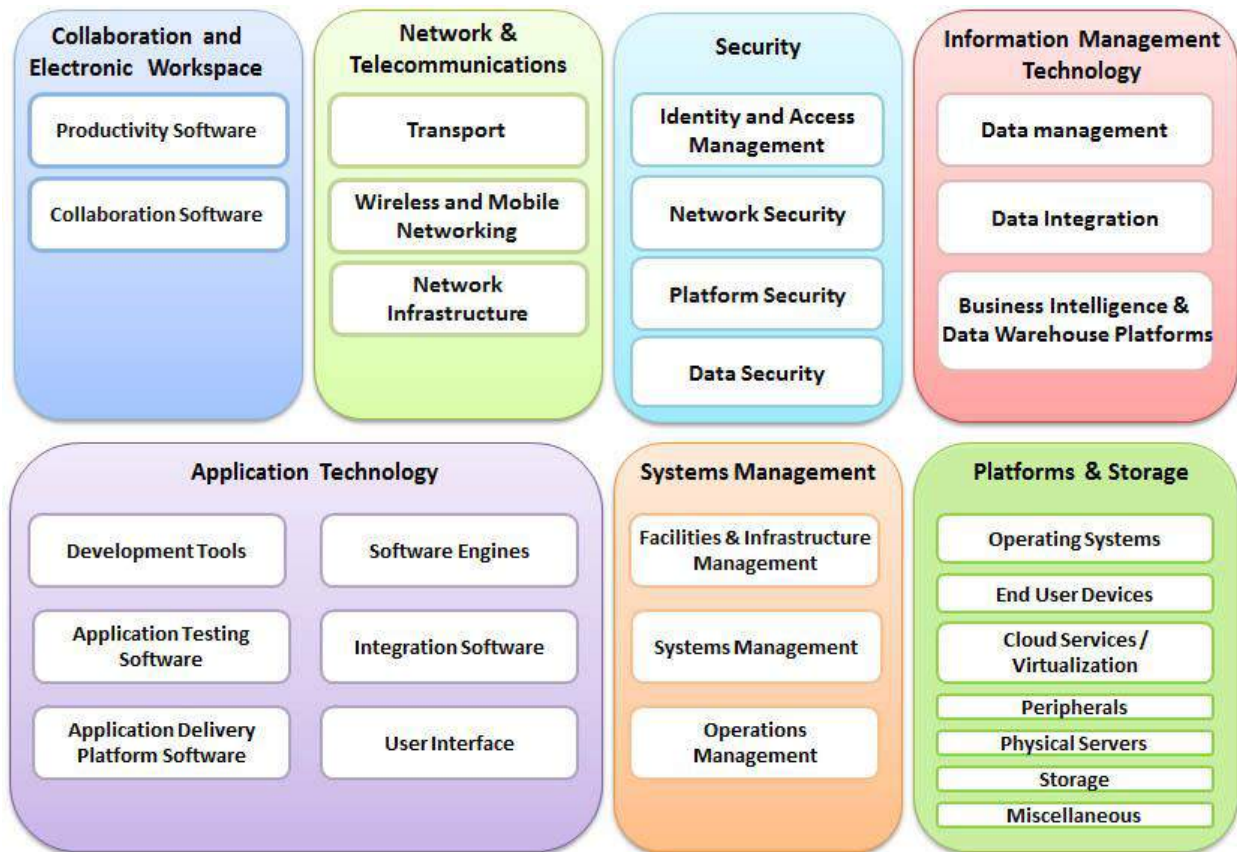


Figure 14 – Technology Categories³⁸

OIT acts as a steward for all VA’s IT assets and resources in this framework. 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.

³⁸ Information Technology (IT) Roadmap Target State Vision of the VA ETA, V.2.15, December 28, 2012



OIT's stewardship of VA's IT infrastructure supports multiple OIT objectives. Under OIT Goal 1, for instance, OIT's IT infrastructure efforts promote: advocating a unified vision of information resource management (1.1), managing the IT portfolio (1.2), delivering an integrated, interoperable VA mission systems environment (1.3), and driving duplication and redundancy out of the VA mission systems environment (1.4). OIT's efforts also support OIT Goal 2 objectives: developing and delivering integrated, innovative, and accessible solutions (2.1); and providing reliable delivery of adaptable, high quality information and technology infrastructure and services (2.2). OIT's work on IT infrastructure similarly supports CIO Strategic Priorities for Next Generation Information Security, Product Delivery, Transparent Operational Metrics, and Fiscal Management.

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*³⁹ 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
- 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 and optimizing unit cost
- 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 both communicates and computes
- Move to VA Cloud Computing where economically justified

³⁹ *Office of Information and Technology FY15-19 Planning Guidance*, February 7, 2013



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 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 resulting from emerging technologies.

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 health care IT, VA is expanding the strategic focus to the external marketplace as a supplier of information systems, as one 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 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)

As envisioned in the FY 2013 OIT Information Technology Roadmap, fifty percent of all new IT infrastructure investments in the near to mid-term 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 funding to be focused on the "To Be" and twenty-five percent of funding spent on sustainment of "As Is" existing technologies.⁴⁰

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 to 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
- Establish a VA-wide "bring your own device" strategy and approach

⁴⁰ VA OIT Information Technology Roadmap, Draft 2.14, December 5, 2012



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 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 aggregating the schedules and cross-project dependencies for each IPL project
- 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 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 drawn from across OIT as well as VA Administrations and staff offices to ensure 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 FY 2011 sustainment lines of approximately \$1.6B to produce a cost analysis by spend category and a lifecycle cost analysis of items purchased
- Online Analytical Processing Analysis – Analyze current VA analytical reporting (business intelligence) capabilities by identifying data redundancy and poor file and table design practices
- Online Transaction Processing 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 VA. 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 across the enterprise.

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 also 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 the VA's efforts to provide a Veteran-centric environment as well as realize efficiencies in its operations. VA is working to provide SOA design patterns 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 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 services
- Promote collaboration with DoD, open source community, and other providers of shared services

5.2.1 Enterprise Shared Services Target State

VA's ESS target state is depicted in Figure 15 below, which is derived from the Open Group's SOA Reference Architecture.⁴¹ The Shared Service target state contains 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; and establishing working group and sub-groups for Governance, Architecture, Capabilities, and Assessments
- Assess agency Shared Service adoption and maturity through a roadmap concept

⁴¹ The Open Group, *SOA Reference Architecture*, ISBN: 1-937218-01-0, November 2011



The diagram below is presented to show the interrelationships between the operational, services, business process, interface, integration, quality, information, and governance layers of the target architecture.

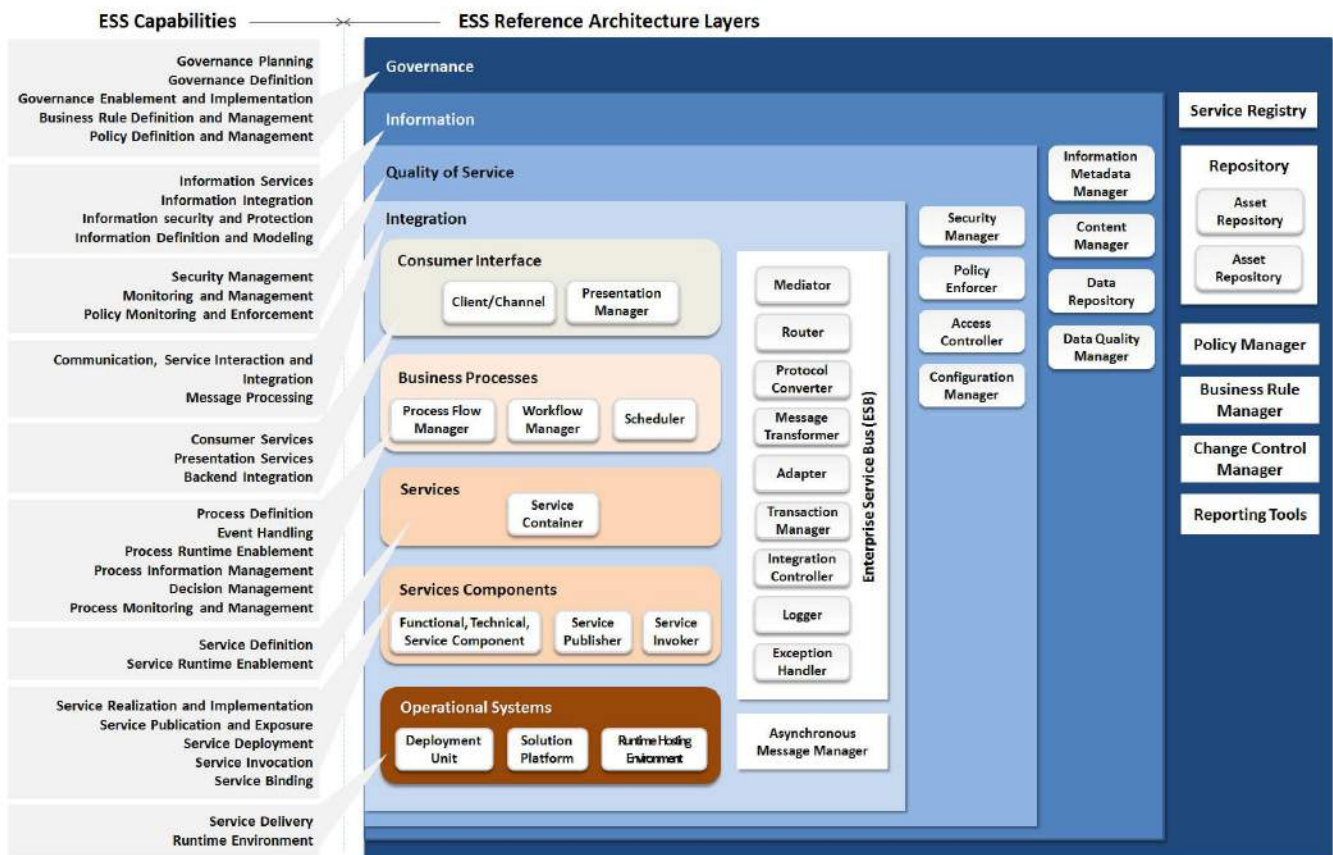


Figure 15 – ESS Reference Architecture



6 Cyber Security, Privacy, and Business Continuity

6.1 Mission and Goals

The OIS within OIT has full responsibility for 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 all stages of Veteran care by protecting the personal information of Veterans and the employees who serve them."*⁴²

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, Homeland Security Presidential Directive 12 (HSPD-12) implementation, and protect the privacy of PII and sensitive but unclassified (SBU) information.

OIS work on data and information security directly supports the CIO's strategic priority on Next Generation Information Security, as well as OIT Objective 2.3, to provide robust and comprehensive information security and privacy services.

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,

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.

⁴² OIS Overview, http://www.ois.oit.va.gov/OIS_Overview.asp



standard security controls, and VA directives are published in the 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 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 mission, goals, and objectives, which align to 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).

The 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. These analyses 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 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 and has resulted in significant remediation of many of the deficiencies that compromise its material weaknesses 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 (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 453,000), it addresses vulnerabilities discovered on those machines.⁴³ 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. In late FY 2012, OIS began integration of the Governance, Risk, and Compliance tool to incorporate prior Visibility to Desktop feeds, Visibility to Server feeds, and other VA security tools into one graphical dashboard. The tool is now being leveraged during the Assessment and Authorization process and will provide information used to determine the security posture of the Department.

6.3.2.1 HSPD-12 Implementation

Since the beginning of its HSPD-12 implementation efforts, 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, VA employees and contractors that work in the VA 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 2.0 (NCPS; formerly known as Einstein) devices are deployed in all four VA Trusted Internet Connection (TIC) Gateways. NCPS Einstein 3 Accelerated (E3A) monitoring of Domain Name System (DNS) is currently operational at one TIC Gateway; the remaining three will be implemented in Q3 FY14. 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.⁴⁴ VA remains committed to the implementation of all critical requirements. VA is approved to operate as a TIC Access Provider (TICAP) for VA's four Internet gateways (Sterling, Virginia; Dallas, Texas; Chicago, Illinois; and San

⁴³ DOJ CIO Dashboard, <http://dashboard.tic.va.gov/s/ST/>

⁴⁴ VA Office of Information Security 2012 Annual Report



Jose, California) and meets all federal requirements for TIC service providers. The TIC gateways continue to improve the security of the VA enterprise network by instituting common security controls and configurations as well as installing additional monitoring capabilities.

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 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)* inform 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 and reported to the Data Breach Core Team and the CIO.

Lastly, VA Directive 6508, *Privacy Impact Assessments* and accompanying VA Handbook 6508.1, *Privacy Impact Assessment*, 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.⁴⁵

Stage 1: Identifies and maps OIT information system contingency planning requirements through development of a business impact analysis, 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

⁴⁵ 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 IT 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 16, also identify training needs for professional development and support OIT's overall efforts to build a future ready workforce (thereby supporting the OIT objective to foster an accomplished, diverse, and empowered workforce aligned to VA mission objectives (3.2)).⁴⁶



Figure 16 – Competency Model Overview

⁴⁶

<http://vaww.infoshare.va.gov/sites/ittrainingacademy/commodel/SharedDocuments/VAOITCompetencyModelImage.pdf>



By using these 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 the VA on-line education training system, Talent Management System. OIT ITWD will continue to add a variety of up-to-date training events for 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 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 include: 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 Department.

7.1.1 OIT Workforce Strategic Alignment (FXXA)

OIT conducted extensive human capital research, planning, and coordination resulting in the development of the *FY 2014-2020 OIT Human Capital Strategic Plan (HCSP)*. The plan was developed by OIT's Human Capital Strategic Working Group, with mentoring and guidance from the VA Office of Human Resources Management Strategic Human Capital Planning Service, which recently drafted the *2014-2020 Draft Transforming Human Capital at VA Strategic Plan*. The *HCSP* is linked to VA *Strategic Plan* Goal 3, Objective 1 (*Make VA a Place People Want to Serve*), and the performance measures and milestones outlined in the Human Capital Assessment and Accountability Framework. Additionally, the *HCSP* was synchronized with OIT subordinate



organization human capital goals and objectives. The plan was finalized and released in October 2013.

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. VA's overall strategy for accessibility is incorporated in VA's policies, outreach and awareness, and measureable deliverables.

The following identifies how VA currently integrates accessibility and Section 508 considerations into processes to develop, procure, maintain, and generally use 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. The 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 the VA 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**

The *VA 2013-2015 Enterprise Roadmap* is provided as a separate document.



Appendix B: OMB M-13-09 Reporting Codes⁴⁷

OMB uses the codes listed in this section to identify specific content in IRM Strategic Plans across all Federal agencies that addresses topics of particular interest to OMB.

- **Agency Strategic Goals and Objectives**
 - Identify agency strategic goals and objectives supported by the IRM strategic plan **(AXXA)**; and
 - Describe how activities of the IRM Strategic Plan and Enterprise Roadmap advance these goals and objectives **(AXXB)**.

- **Improving Services to Customers**
 - Describe how your agency regularly evaluates existing and planned customer-facing services to:
 - Measure customer use and satisfaction through analytics and other approaches **(BXXA)**;
 - Improve usability, availability, and accessibility of services, including optimization of services for mobile use **(BXXB)**; and
 - Advance agency performance goals **(BXXC)**.

- **Governance and Management Processes**
 - Describe the governance process the agency uses to ensure that current law and policy are followed when planning, prioritizing, funding, executing, and decommissioning IT investments. If there are differences in the way the governance process is implemented across organizational units, describe those differences and why they exist. At a minimum, address:
 - The scope of the governance process, including Investment Review Board and other Portfolio Governance Boards (as appropriate) along with delegation of authority to bureaus or other organizational units (as appropriate) **(CXXA)**;
 - Which agency stakeholders are engaged, including "C"-level leadership **(CXXB)**;
 - The valuation methodology used to comparatively evaluate investments, including what criteria and areas are assessed **(CXXC)**;
 - How the agency ensures investment decisions are mapped to agency goals and priorities **(CXXD)**;

⁴⁷ OMB Memorandum M-13-09, *Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management*, March 27, 2013



- A high-level description of the process used to assess proposed investments and make decisions, including frequency of meetings and how often the process is updated **(CXXE)**;
 - How you coordinate between investment decisions, portfolio management, enterprise architecture, procurement, and software development methodologies **(CXXF)**; and
 - Describe the agency's IT strategic sourcing plan, to include processes for addressing enterprise licenses **(CXXG)**.
- **CIO Authorities**
 - Describe how the agency policies, procedures and authorities implement CIO authorities, consistent with OMB Memorandum 11-29, "Chief Information Officer Authorities" **(DXXA)**.
 - **Cybersecurity Management**
 - Summarize your agency's strategy to ensuring that IT investment and portfolio decisions align with the Administration's [White House's] Cybersecurity Priority Capabilities and your agency's IT security goals, and how you will continue to strengthen this alignment **(EXXA)**; and
 - Describe your agency's approach to ensure all mission critical applications have the proper continuity of operation and disaster recovery capabilities such that the agency can support the proper level of continuity of Government operations in accordance with Federal statute and guidance **(EXXB)**.
 - **Workforce**
 - Summarize your agency's approach to IT human capital planning, including the ability to build a future ready workforce to support the agency's strategic goals and objectives **(FXXA)**.
 - **Managing Information as an Asset**
 - Include how your agency will promote interoperability and openness throughout the information life cycle and properly safeguard information that may require additional protection.
 - Specifically address how information collection and creation efforts, information system design, and data management and release practices will support interoperability and openness **(GXXA)**.



- Describe how your agency ensures that personal information, including personally identifiable information (PII) and controlled, unclassified information (CUI), is accessible only to authorized personnel and how frequently these controls are verified **(GXXB)**.
- **Commodity IT and Shared Services**
 - Describe your agency's approach to maturing the IT portfolio, to include optimizing commodity IT (including data centers), rationalizing applications and adopting a service orientation approach **(HXXA)**;
 - Describe the agency's plan to re-invest savings resulting from consolidations of commodity IT resources (including data centers) **(HXXB)**; and
 - Describe your agency's approach to maximizing use of inter-and intra-agency shared services (such as those enabled by common platforms and lines of business) and shared acquisition vehicles for commodity IT, such as those determined by the Strategic Sourcing Leadership Council, in order to reduce duplicative contract vehicles **(HXXC)**.
- **Accessibility**
 - Describe the agency's approach to:
 - Creating a diverse environment where individuals of all abilities can work, interact, and develop into leaders **(IXXA)**;
 - Integrating accessibility considerations into the processes used in developing, procuring, maintaining, or using IT **(IXXB)**; and
 - Building workforce skills to support an environment where Section 508 requirements and responsibilities are well understood, communicated, implemented, and enforced **(IXXC)**.



Acronyms

Acronym	Definition
APG	Agency Priority Goal
APMF	Acquisition Program Management Framework
API	Application Programming Interface
AS/IT	Assistant Secretary for Information and Technology
ASD	Architecture, Strategy, and Design
BOP	Business Operating Plan
CA	Customer Advocate
CDI	Customer Data Integration
CIO	Chief Information Officer
CUI	Controlled, Unclassified Information
DoD	United States Department of Defense
DRP	Disaster Recovery Plan
E2ERM	End-to-End Requirements Management
EA	Enterprise Architecture
ELT	Executive Leadership Team
ERM	Enterprise Risk Management
ESS	Enterprise Shared Services
ETA	Enterprise Technical Architecture
FDGS	Federal Digital Government Strategy
FOC	Full Operational Capability
FOM	Functional Organizational Manual
FY	Fiscal Year
GAO	Government Accountability Office
GPRA	Government Performance and Results Act
HCSP	FY 2014-2020 OIT Human Capital Strategic Plan
HSPD-12	Homeland Security Presidential Directive 12
IAM	Identity and Access Management
iEHR	Integrated Electronic Health Record
IOC	Initial Operational Capability
IPL	Integrated Priority List
IPO	Interagency Program Office
IRM	Information Resources Management
ISCP	Information System Contingency Plans
IT	Information Technology
ITLB	Information Technology Leadership Board
ITRM	IT Resource Management
ITWD	IT Workforce Development
MARA	Mobile Application Reference Architecture
MPR	Monthly Performance Review



Acronym	Definition
MYP	Multi-Year Programming
NIST	National Institute of Standards and Technology
OEC	Office of Enterprise Communications
OIA	Office of Informatics and Analytics
OIS	Office of Information Security
OIT	Office of Information and Technology
OMB	Office of Management and Budget
OMR	Operational Management Review
OOR	Office of Responsibility
OPP	Office of Policy and Planning
PD	Product Development
PDF	Portable Document Format
PGD	Patient Generated Data
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PMAS	Project Management Accountability System
PPBE	Planning, Programming, Budgeting, and Execution
PPBEB	Planning, Programming, Budgeting, and Execution Board
PR	Performance Review
QPO	Quality, Performance and Oversight
RRTF	Ruthless Reduction Task Force
SBU	Sensitive But Unclassified
SDE	Service Delivery and Engineering
SEP	Stakeholder Enterprise Portal
SIT	Strategic Investment Tool
SMC	Strategic Management Council
SOA	Service Oriented Architecture
SPI	Sensitive Personal Information
SRG	Senior Review Group
TIC	Trusted Internet Connection
V2E	Visibility to Everything
VA	United States Department of Veterans Affairs
VAEB	VA Executive Board
VDC	Veteran Online Application (VONAPP) Direct Connect
VHA	Veterans Health Administration
VistA	Veterans Health Information Systems and Technology Architecture
VRM	Veterans Relationship Management
VSO	Veterans Service Organization



Bibliography/References

- DOJ, CIO Dashboard, <http://dashboard.tic.va.gov/s/ST/>
- Office of Management and Budget, *Digital Government: Building a 21st Century Platform to Better Serve the American People* (May 23, 2012)
- OMB, Memorandum M-12-10, *Implementing PortfolioStat*, March 30, 2012
- OMB, Memorandum M-13-09, *Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management*, March 27, 2013
- *Personnel and Accounting Integrated Data (PAID) Report*, February 28, 2014
- *Program Management Summit, Acquisition Program Management Framework (APMF) Implementation*, January 29, 2014
- Program Management Summit, *Performance Excellence, The Baldrige Criteria, and The Program/Project Manager*, January 29, 2014
- *Report to Congress on Implementation of The E-Government Act of 2002 (FY2009)*
- SDE asset management tracking, March 28, 2014
- *The Open Group, SOA Reference Architecture*, ISBN: 1-937218-01-0, November 2011
- VA, *CIO Annual 2012 Performance and Accountability Report FY12*, November 15, 2012
- VA, *CIO Annual Report FY 2012 (DRAFT)*
- VA, *VA Information Technology Planning, Programming, Budgeting, and Execution Board (IT PPBEB) Draft Charter, Draft V.5.4*, November 8, 2012
- VA, *Digital Government Strategy Report for the Department of Veteran Affairs*, May 5, 2013
- VA, Directive 0323, *VA Continuity Program*, November 5, 2010
- VA, Directive 6051, *VA Enterprise Architecture (EA)*, July 21, 2002
- VA, *Functional Organizational Manual – Version 1.1*, October, 2013
- VA, *FY2012 OIS Annual Report*, October 2012
- VA, *Information Technology (IT) Roadmap Target State Vision of the VA Enterprise Technical Architecture (ETA)*, V.2.15, December 28, 2012
- VA, *IT Portfolio Management Process Maturity Overview*, PowerPoint presentation, June 12, 2012
- VA, *IT Strategic Plan FY 2012-2015*, November 2012
- VA, Memorandum, *Office of Information and Technology (OIT) Fiscal Year (FY) 2015-2019 Planning Guidance*, March 12, 2013



- VA, *Office of Information and Technology FY15-19 Planning Guidance*, February 7, 2013
- VA, *Office of Information Security 2012 Annual Report*
- VA, OIA PDG Project Database, July 2013
- VA, *OIS Overview*, http://www.ois.oit.va.gov/OIS_Overview.asp
- VA, *OIT Information Technology Roadmap V.2.14*, December 5, 2012 (DRAFT)
- VA, PAID Human Resources Data, March 31, 2013
- VA, *Performance Excellence, The Baldrige Criteria, and The Program/Project Manager*, presentation at Program Management Summit, January 29, 2014
- VA, *PMAS Guide 4.0*, November 17, 2012
- VA, *VA OIT FY 2014 President's Budget*
- VA, *VA Open Government Plan*, June 2010
- VA, *VA Planning Guidance (FY) 2016-2020 Memorandum*, September 27, 2013
- VA, PortfolioStat 2012 Overview, Government Accountability Office (GAO) briefing, April 22, 2013
- VA, *Programming Guidance Fiscal Year 2016-2020 PPBE Cycle*, October 11, 2013
- VA, Strategic Management Council (SMC), Acquisition Program Management Framework (APMF) Update, May 1, 2013
- VA, Strategic Planning Team Briefing 09_12_13 Final, September 12, 2013
- VA, *Strategic Plan Refresh FY 2011-2015*
- VA, *VA Strategic Plan FY 2014-2020*, accessed on March 6, 2014
- VA, *VistA Evolution Program Plan*, version 1.20, October 24, 2013
- VA, *Welcome to ITRM Manual*, ITRM Functional Statement, June 2011
- http://vaww.infoshare.va.gov/sites/ittrainingacademy/compmodel/SharedDocuments/VA_OITCompetencyModelImage.pdf