

**STATEMENT OF MS. LAVERNE COUNCIL
ASSISTANT SECRETARY FOR INFORMATION TECHNOLOGY AND
CHIEF INFORMATION OFFICER
DEPARTMENT OF VETERANS AFFAIRS
Before the House Committee on Oversight and Government Reform
Subcommittee on Information Technology
March 16, 2016, at 2:00 p.m.**

Good afternoon, Chairman Hurd, Ranking Member Kelly, and distinguished members of the Subcommittee. Thank you for providing me with this opportunity to discuss the progress that the Department of Veterans Affairs' (VA) Office of Information and Technology (OI&T) is making towards better serving our VA business partners and our Nation's Veterans.

INTRODUCTION

VA at a Turning Point

VA recognizes that persistent internal challenges exist in delivering services across key areas. We have listened to concerns from the Veterans we serve, as well as their representatives in Congress.

To foster a continual and productive conversation with Congress, we meet with our committees of jurisdiction on a recurring basis, and welcome opportunities, such as this, to meet with other Members of Congress. We are continuing to work closely with the Department of Defense (DoD) to make the transition to Veteran status go as smoothly as possible. We have also looked inward and benefited from the shared experiences of numerous VA officials.

As we implement recommendations from our stakeholders, we are working to stay ahead of numerous factors that affect how we do business.

- **Changing Veteran demographics:** Aging Veterans are seeking and using benefits (e.g., long-term care) at significantly higher rates.
- **Shifting business partner needs:** OI&T is dealing with new and increasingly diverse customer needs and must provide increasingly complex information technology (IT) support (e.g., Telehealth).
- **Rising expectations:** Members of Congress and the American people are closely scrutinizing how well the VA is delivering health services to Veterans.
- **Growing cyber threats:** The persistent risk of cyber-attacks—combined with continuing digitization of health care—increases exposure, vulnerability, and potential consequences of a data breach.
- **Next generation IT delivery models:** External IT delivery models are constantly evolving, with increasing adoption of services and more commercial-style techniques (e.g., learning by doing).

- **Consumerization of IT:** The IT landscape emphasizes a real-time, mobile-first, hyper-targeted digital experience, with customers increasingly demanding the same experiences in the workplace.
- **Internet of Things:** The rapidly growing number of sensors and actuators connected by networks to computing systems are now driving innovation on patient care.

These issues are too complex to solve with quick fixes and addressing them requires nothing short of a transformation.

When I testified on October 27, 2015, I shared our IT Enterprise Strategy with the Committee. The IT Enterprise Strategy provides a roadmap for our ongoing transformation. The strategy has a new mission, vision, guiding principles, and strategic goals, and I am proud to share these with you today. Our new mission is to collaborate with our business partners to create the best experience for all Veterans. Our vision is to provide a seamless, unified Veteran experience through the delivery of state-of-the-art technology. Our guiding principles are to be transparent, accountable, innovative, and team-oriented. Our strategic goals, which align with strategic plans across VA, are to stabilize and streamline core processes and platforms, eliminate material weaknesses, and institutionalize a new set of capabilities to drive improved outcomes.

VA plans to achieve our goals through a prioritized set of strategic initiatives across our “Now, Near, and Future” time horizons.

Importance of OI&T to VA’s Infrastructure

VA must have an exemplary IT organization to provide the highest level of service to our Veterans. IT is an enabler of each of VA’s disparate lines of business, including the largest integrated health care system in the United States; a benefits processing organization equivalent to a medium-size insurance company; one of the largest integrated memorial and cemetery organizations in the country; and many other components.

We are establishing a strong technical foundation that ensures alignment with VA’s mission, data visibility, and accessibility; data interoperability; infrastructure interoperability; information security; and enterprise services.

This transformation is different. We are measuring success, ensuring accountability, investing in the capabilities of OI&T employees, and collaborating across VA to build trust.

We are adopting a customer-centric mindset throughout the end-state design process, including collaborative engagement with all key stakeholders. We are institutionalizing a “buy-first” strategy that leverages existing commercial solutions first before building

internally. Finally, we are incorporating best practices from the public and private sector to spur agility, efficiency, effectiveness, and innovation in service delivery.

VA is also working to create a holistic view of the Veteran to improve their experience, care, and benefits. Currently, we can view the full-service record at any time prior to or after separation. Our goal for the future is to seamlessly create and maintain a secure and accurate enterprise record in support of our Veterans.

Today, I am pleased to share with the Committee our progress in implementing the Federal Information Technology Acquisition Reform Act (FITARA) objectives. The first steps of our transformation include establishing the Enterprise Program Management Office (EPMO) and creating the Enterprise Cybersecurity Strategy.

Enterprise Program Management Office

EPMO is building our momentum. EPMO hosts our biggest IT programs, including VistA Evolution, Interoperability, the Veterans Benefits Management System, and Medical Appointment Scheduling System. In addition, EPMO improves project portfolio, resource tracking, and communication around these programs and projects. EPMO also supports FITARA requirements.

The EPMO is led by the Deputy Assistant Secretary for EPMO, who reports to me, and this position complies with FITARA Requirement 831, *CIO Oversight*.

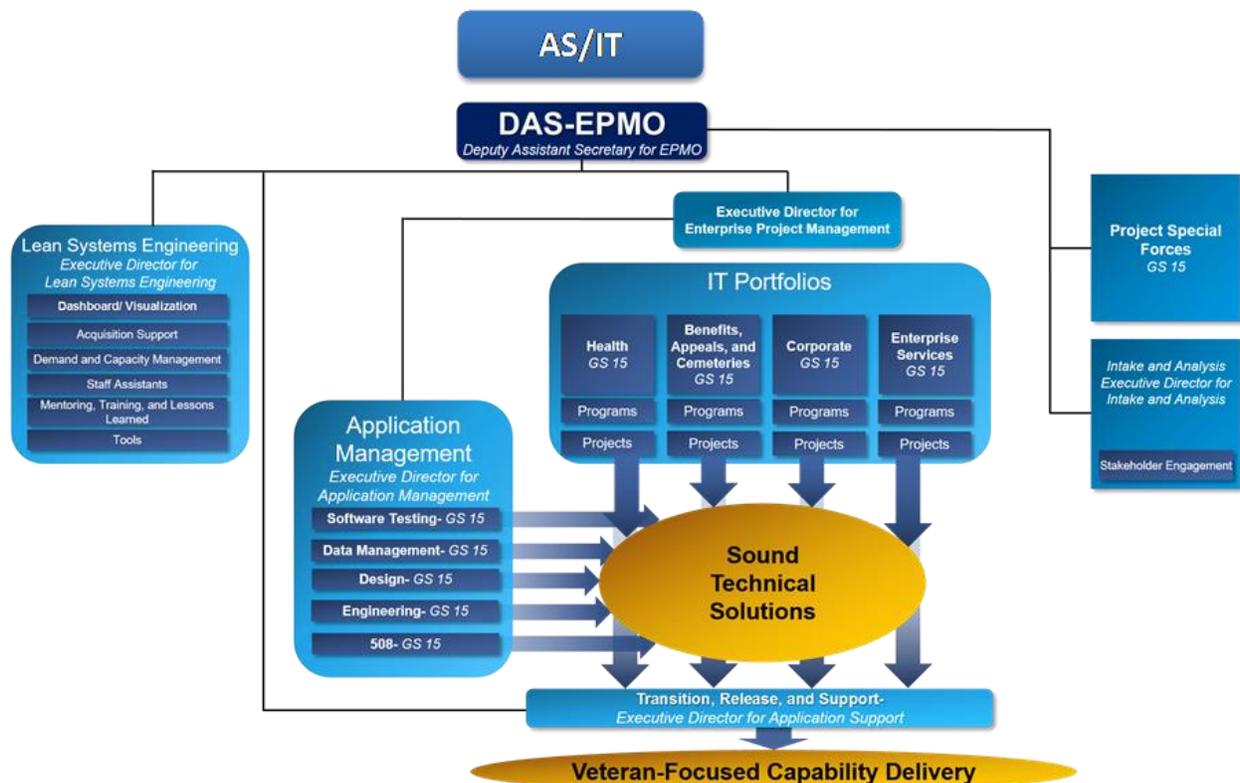


Fig. 1 – EPMO Organizational Chart

Here is a breakdown of how our EPMO functions help VA meet FITARA requirements:

The **Intake and Analysis of Alternatives** function works with business lines, including the Veterans Health Administration (VHA), the Veterans Benefits Administration (VBA), and the National Cemetery Administration (NCA), to: develop requirements to meet the needs of Veterans, provide analyses of alternatives, provide risk assessments/ratings, determine program initiation, and integrate security from the onset.

This function supports the following FITARA requirements:

- Congressional/public reporting(832)
- Risk assessments/ratings (832)
- Review of portfolio of IT investments (833)
- Federal Strategic Sourcing Initiative and Government-wide Software Purchasing Program (836 and 837)
- Cybersecurity (834)

The **IT Portfolios** function consolidates programs and projects under five VA IT portfolios (Health, Benefits, Cemeteries, Corporate, and Enterprise services), and integrates security into all aspects of these projects.

The **Project Special Forces** function rescues projects at risk of failure. This function supports the following FITARA requirements:

- Risk assessment/management (832)
- Techstat Sessions (832)

The **Lean Systems Engineering** function manages dashboard/visualization (metrics gathering and analysis), development process tools, contracting/acquisitions administration, budget execution/human resources, and training. This function supports the following FITARA requirements:

- Metrics, Cost Savings, and Avoidance (833)
- Risk assessment/management (832)

The **Transition Release and Support** function transitions product sustainment to Service Delivery and Engineering for sustainment operations and manages the integrated calendar (POLARIS) across OI&T. This function supports the following FITARA requirements:

- Metrics, Cost Savings, and Avoidance (833)
- Risk assessment/management (832)

The **Application Management** function manages IT implementation efforts, including testing, design, and data management within EPMO. This function supports the following FITARA requirements:

- Risk assessment/management (832)
- Cybersecurity (834)

EPMO ensures alignment of program portfolios to strategic objectives and provides visibility and governance into the programs. EPMO also allows for better analysis of and reporting on programs, projects, resources, and timelines to optimize the best combination of each. This helps ensure the overall health of portfolios through reporting and analysis of portfolio performance metrics.

For enterprise initiatives, EPMO helps program and project teams to better develop execution plans, monitor progress, and report the status of these programs and projects. EPMO enables partnerships with IT architects for enterprise collaboration and serves as a program/project resource for the delivery of enterprise and cross-functional programs. This helps identify Shared Services Enterprise Programs and will help plan resource requirements with portfolios and architecture.

EPMO improves communication by better managing internal and external communication and employee engagement. EPMO also enables the coordination of enterprise communications by developing comprehensive, enterprise communication strategies to drive consistency of messaging.

EPMO has already produced results. The Veteran-focused Integration Process (VIP) is a project-level based process that replaces the Project Management Accountability System (PMAS). VIP establishes a single release process with a predictable cadence that all VA organizations will follow by the end of 2016. It reduces overhead and eliminates redundancy in review, approval, and communication processes. These efficiencies include reducing the review process from 10 independent groups with 90 people to a single group of 30 people focused on ensuring that products meet specified, consistent criteria for release.

VIP focuses on doing rather than documenting, with a reduction of artifacts from over 50 to just 7, plus the Authority to Operate (ATO) and the shift from a 6-month to a 3-month delivery cycle. VIP establishes two critical decision points as part of the Project and Product Phases to determine if a project is viable and if a product is ready for production release, replacing the five-phase gates/milestones from PMAS. Further, as a guarantee to our work, EPMO will ensure that product teams stay assigned to their projects for at least 90 days after the final deployment.

POLARIS, or the enterprise-unified calendar, is the consolidation of six separate calendars from across the enterprise. POLARIS will serve as OI&T's unified calendar in support of the VIP framework. After identifying a release date for a product, OI&T will enter an initial calendar entry or update into POLARIS during the execution phase of the VIP lifecycle.

FITARA Progress

Budget Formulation and Planning

Rating	Description
(1) Incomplete	Agency has not started development of a plan describing the changes it will make to ensure that all baseline FITARA responsibilities are in place by December 31, 2015.
(2) Partially Addressed	Agency is working to develop a plan describing the changes it will make to ensure that all baseline FITARA responsibilities are in place by December 31, 2015.
(3) Fully Implemented	Agency has developed and implemented its plan to ensure that all common baseline FITARA responsibilities are in place.

Table: FITARA Self-Assessment Rating Scale

A1 and A2: Visibility of Information Technology (IT) Resources (Rated 2 out of 3)

FITARA requires that the Chief Information Officer (CIO) be significantly involved in the budget process to ensure that IT resources are visible in the budget. Currently, as part of FITARA's system of self-reporting, VA rates itself a two; however, we are evaluating all programs along a new framework, allowing us to better understand the budget and spending. The new framework will provide a clear line of sight into the budget at each phase of the process—before plan, after plan, during an active state, and at completion.

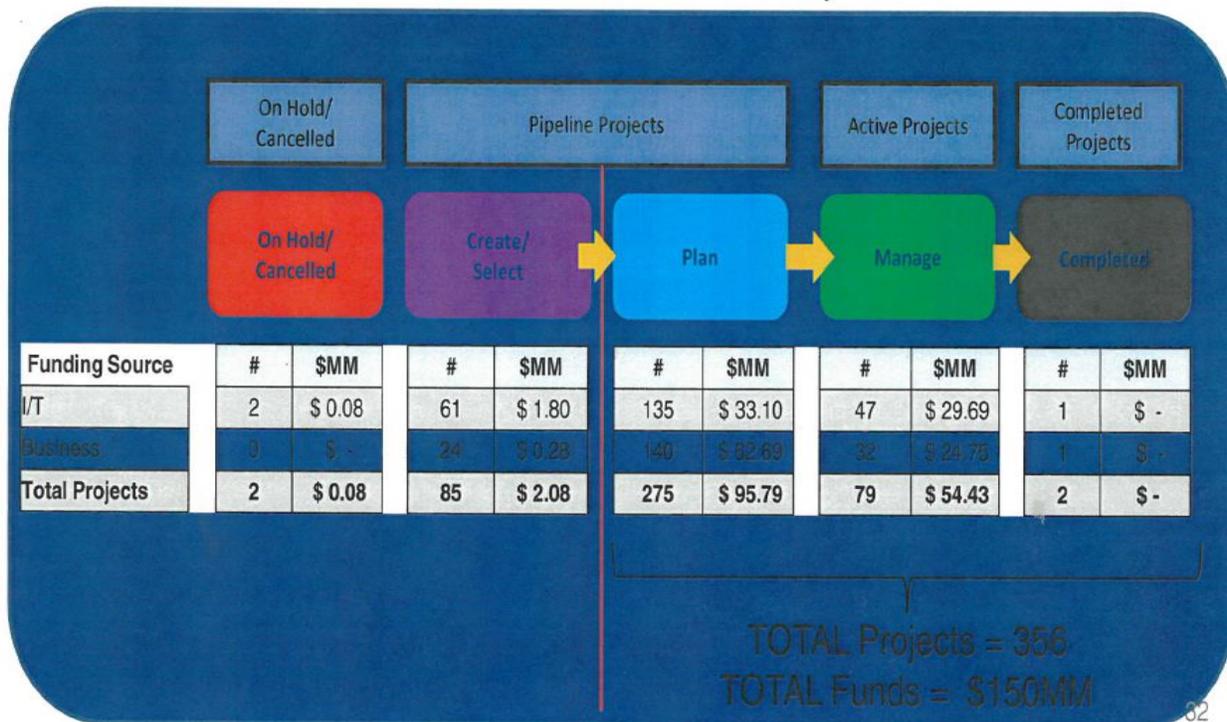


Fig. 2 – Sample Project Framework Pipeline

As VA's CIO, I take an active role in the budgeting process to ensure the visibility of IT resources in budget formulation and planning. However, IT appropriation is not the only source of funding for all IT-related activities. For example, medical devices that connect to VA networks have never been a part of the IT appropriation. As the scope of what is IT-related has increased in the years since the IT appropriation was established, the range of items not covered by the IT appropriation has increased. Typically, this category includes physical devices.

VA is working to ensure that all IT-related purchases require CIO approval and are fully compliant with OI&T policy, rules, and standards. EP MO will be responsible for the overall IT portfolio management processes within VA, subsuming the role of the IT Planning, Programming, Budget, and Execution (PPBE) Board. IT account managers will have a dotted-line reporting relationship to their respective undersecretary and be responsible for the overall vision of information management/IT capabilities supporting the Administrations, the assessment of all Administration-specific business requirements and their translation into IT requirements, and the advocacy of all Administration-specific requirements in the budget prioritization and formulation process. We are on track to have this policy in place by April 30, 2016.

OI&T's account manager structure is being recognized throughout the Department as a best practice, with other VA organizations beginning to set up similar account management structures. The following are the OI&T account manager portfolios:

- The Account Manager for Corporate IT manages the Supply Chain, Appeals, Staffing, and Leaders Developing Leaders accounts;
- The Account Manager for Health Clinical Facing functions manages the Homelessness and Access accounts;
- The Account Manager for Benefits and Back Office Health manages the Care in Community, Compensation and Pensions, Contact Centers, Veterans Crisis Line, and Unified Veterans Experience accounts; and
- I manage the Improve Veterans Experience, and OI&T Transformation accounts.

B1 and B2: CIO role in pre-budget submission (Rated 2 out of 3)

FITARA requires the CIO to take an active role in pre-budget submission. VA rates itself a two, partially addressing this requirement with plans to fully address the requirement.

EPMO's governance will replace OI&T's PPBE. EPMO and Account Managers will provide information necessary to gauge project and program performance to the IT Leadership Board and VA Executive Board. The IT Leadership Board and VA Executive Board can proactively terminate obsolete or unsuccessful programs or projects ahead of the budget submission, thereby reducing costs and freeing up resources for more effective programs.

C1 and C2: CIO role in planning program management (Rated 3 out of 3)

FITARA requires the CIO be involved in internal planning processes for using IT resources. VA rates itself a three, fully addressing the requirements.

The CIO is a direct report to the Deputy Secretary of Veterans Affairs. In addition, the CIO sits on the VA Executive Board. The CIO is the executive-in-charge of all decisions associated with the execution of the IT appropriation and advises the Secretary and Deputy Secretary regarding execution of this appropriation.

The Enterprise Architecture (EA) team, reporting to the OI&T Deputy Assistant Secretary for Architecture, Strategy, and Design (ASD), is directly involved in developing the VA Strategic Plan. This engagement involves performing environmental scans, identifying significant global trends, analyzing trends to assess their potential long-term significance (10 to 20 years in the future), defining possible futures, assessing the impacts, and identifying gaps and strategic options. The EA team's involvement ensures that the VA Strategic Plan leverages the opportunities inherent in information capabilities to the maximum extent possible, while representing the CIO's resourcing interests, priorities, and concerns.

D1 and D2: CIO role in budget request (Rated 2 out of 3)

FITARA requires that the CIO must review and approve major IT investment portions of the budget request. VA rates itself a two, partially addressing this requirement with plans to fully address the requirement.

The CIO manages a centralized IT account and submits a budget request that includes all IT requirements to the Office of Management and Budget (OMB). VA's Chief Financial Officer and Chief Acquisition Officer (CAO) participate throughout the budget process.

Acquisition and Execution

E1 and E2: Ongoing CIO engagement with program managers (Rated 2 out of 3)

FITARA requires the CIO to engage on a regular basis with agency officials to evaluate IT resources available to programs and make sure that all programs have appropriate levels of IT support. VA rates itself a two, partially addressing this requirement with plans to fully address the requirement.

VA has established and executes the delivery of IT capabilities under the PMAS project and program management framework. PMAS's successor, VIP, is the follow-on framework for IT development at VA. This will unify and streamline IT delivery oversight and deliver IT products more efficiently, securely, and predictably. Importantly, VIP will reduce required documentation by two-thirds, decrease the number of gates from five to two, and reduce the overall cycle time from six to three months.

PMAS	
Document Driven (58 Documents)	Data Driven (7 Documents + ATO)
5 Phase Gates/Milestones	2 Critical Decision Events
Multiple Release processes	1 Integrated Release process
6 month delivery cycle	3 month delivery cycle
Ad-hoc hierarchy of programs and projects	Portfolio-based management
Waterfall Centric	Agile Centric
Security + Architecture late in the process	Security + Architecture standards leveraged early, during planning
Project-centered (tactical)	Portfolio-centered (strategic)

Fig. 3 – Improvements from VIP over PMAS

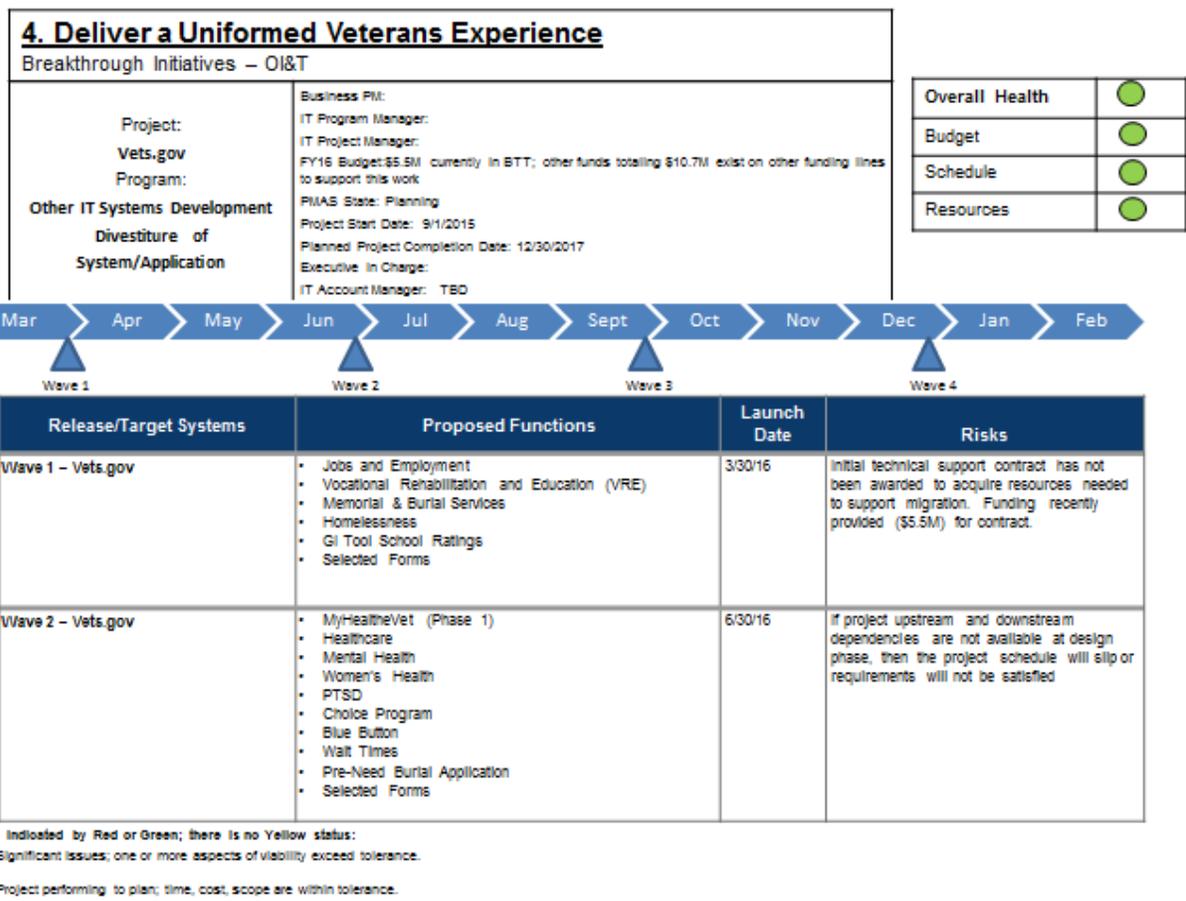


Fig. 4 – OI&T Breakthrough Initiatives

F1 and F2: Visibility of IT planned expenditure reporting to CIO (Rated 2 out of 3)

One of FITARA’s goals is to ensure CIO involvement in agency-wide planned expenditure reporting for all transactions that include IT resources. VA rates itself a two, partially addressing this requirement with plans to fully address the requirement.

VA has a central IT appropriation with participation from the CIO, IT CFO, CAO, and all VA Administrations and Staff Offices as described in Section B of FITARA rules. The CIO and IT CFO manage budget requirements through a governance process that includes collaboration with EPMO.

EPMO enhances the CIO’s visibility into overall project health as it relates to the time, budget, and quality performance as well as alignment to Veteran-centric outcomes. Administration-specific Program Managers will facilitate collaboration, performance measurements, and open lines of communication for the CIO and the Administrations. EPMO will ensure an optimal level of accountability, value, and customer service.

G1: CIO Defines IT Processes and Policies (Rated 2 out of 3)

FITARA requires the CIO to set IT processes and policies. VA rates itself a two, partially addressing this requirement with plans to fully address the requirement.

The PMAS Guide, a VA policy, defines the development processes, milestones, review gates, and the overall policies for all VA IT project management. The PMAS successor, VIP, is the follow-on framework for IT development at VA. VIP will unify and streamline IT delivery oversight and develop IT products more efficiently, securely, and predictably. Importantly, VIP will reduce required documentation by two-thirds, decrease the number of gates from five to two, and reduce the overall cycle time from six to three months.

H1 and H2: CIO Role on Program Governance Boards (Rated 2 out of 3)

FITARA requires the CIO to be a member of program governance boards that utilize IT resources to ensure early matching of appropriate IT with program objectives. VA rates itself a two, partially addressing this requirement with plans to fully address the requirement.

As CIO, I chair the IT Leadership Board and report to the VA Executive Board. However, because some IT-related activities fall outside of the IT appropriation, there is a potential gap in CIO oversight. We are working to revise policy to address this gap.

I1: Shared acquisition and procurement responsibilities (Rated 3 out of 3)

The Federal Information Security Modernization Act (FISMA) requires the CIO to review all cost estimates of IT-related costs to ensure that all acquisition strategies and acquisition plans that include IT apply adequate incremental development principles. VA rates itself a three, fully addressing the requirement.

The PMAS Guide, a VA policy, established guidelines for ensuring that acquisition strategies and plans for IT development projects support incremental development. PMAS's successor, VIP, is the follow-on framework for IT development at VA. VIP will unify and streamline IT delivery oversight and deliver IT products more efficiently, securely, and predictably. Importantly, VIP will reduce required documentation by two-thirds, decrease the number of gates from five to two, and reduce the overall cycle time from six to three months.

J1: CIO Role in Recommending Modification, Termination, or Pause of IT Projects (Rated 3 out of 3)

FITARA requires the CIO to use applicable performance measurements, such as TechStat reviews, to evaluate the use of the IT resources and recommend modification, termination, or pause of IT projects. VA rates itself a three, fully addressing the requirement.

Every project that fails to deliver on its committed delivery date requires a TechStat review. This process falls under PMAS and will continue under VIP. Through a TechStats review, VA's CIO can monitor and evaluate the performance of IT programs of the agency to determine whether a project should continue, be modified, or terminated. This allows VA to determine why the project did not execute and how to set up the project for successful execution in the future. At a TechStat review, senior leaders determine whether a project should be paused, modified, or terminated.

OI&T notifies OMB at least 2 weeks in advance of convening a TechStat review. VA's CIO signs all TechStat review decision memoranda, documenting the actions/decisions at each TechStat review. VA reports results of the TechStat review to OMB through the Integrated Data Collection.

K1 and K2: CIO Review and Approval of Acquisitions (Rated 3 out of 3)

FITARA requires the CIO to review and approve all acquisition strategies and interagency agreements that involve IT resources. VA rates itself a three, fully addressing this requirement.

OI&T requires submission of all products and services, as well as any non-IT products that connect to a VA network operated and maintained by OI&T, or that will or have the potential to store sensitive data into the VA Information Technology Acquisition Request System (ITARS) for review by the CIO.

The ITARS system provides all levels of functionality and authority to support the reporting, editing, certification, and disposition of all VA IT-related requests.

L1 and L2: CIO Approval of Reprogramming (Rated 3 out of 3)

FITARA requires the CIO to approve all funding transfers that involve IT resources and require Congressional notification. VA rates itself a three, fully addressing this requirement.

OI&T has a governance process that ensures the CIO's involvement in the approval of any movement of funds for IT resources that require Congressional notification or approval.

Organization and Workforce

M1 and M2: CIO approves bureau CIOs (Rated 3 out of 3)

FITARA has several requirements related to bureau CIOs. VA does not have bureau CIOs; VA's CIO provides all IT services throughout the Department. VA rates itself a three, fully addressing this requirement.

As CIO, I am responsible for the vision, management, operation, and execution of VA's OI&T and its resources. As VA does not have bureau CIOs, VA's OI&T provides all IT support to VA's Administrations and Staff Offices, and is the only organization within VA authorized to have IT personnel.

N1 and N2: CIO role in ongoing bureau CIO's evaluations (Rated 3 out of 3)

FITARA has several requirements related to bureau CIOs. VA does not have bureau CIOs; VA's CIO provides all IT services throughout the Department. VA rates itself a three, fully addressing this requirement.

As CIO, I am responsible for the vision, management, operation, and execution of VA's OI&T and its resources. As VA does not have bureau CIOs, VA's OI&T provides all IT support to VA's Administrations and Staff Offices, and is the only organization within VA authorized to have IT personnel.

O1 and O2: Bureau IT leadership directory (Rated 3 out of 3)

FITARA has several requirements related to bureau CIOs. VA does not have bureau CIOs; VA's CIO provides all IT services throughout the Department. VA rates itself a three, fully addressing this requirement.

As CIO, I am responsible for the vision, management, operation, and execution of VA OI&T and its resources. As VA does not have bureau CIOs, VA's OI&T provides all IT support VA's Administrations and Staff Offices, and is the only organization within VA authorized to have IT personnel.

P1 and P2: IT Workforce (Rated 2 out of 3)

Under FITARA, VA must develop a set of competency requirements for IT leadership and staff to ensure that the Department can: (a) anticipate and respond to changing mission requirements; (b) maintain workforce skills in a rapidly developing IT environment; and (c) recruit and retain the IT talent needed to accomplish the mission. VA rates itself a two, partially addressing this requirement with plans to fully address the requirement.

OI&T follows a set of competency requirements for all IT leadership and staff. We are refreshing the current Strategic Human Capital Plan and are working on strategic talent recruitment. In addition, we are updating Senior Executive Service (SES) performance plans to align to FITARA elements. We established an OI&T Strategy Human Capital Plan Refresh Working Group in March 2015 to address our workforce requirements and lessons learned, as well as incorporated all FITARA requirements.

CIO Reports to Agency Head (Rated 3 out of 3)

The Clinger-Cohen Act requires that the CIO report directly to the agency head. VA rates itself a three, fully addressing this requirement.

VA's CIO reports directly to and serves as the principal advisor on all matters relating to IT management to the Office of the Secretary of Veterans Affairs through the Deputy Secretary of Veterans Affairs. The VA CIO has direct access to the Secretary regarding programs that include information technology.

Enterprise Cybersecurity Strategy

OI&T is facing the ever-growing cyber threat head on. The first step in our transformation was addressing enterprise cyber security. We delivered an actionable, far-reaching, cybersecurity strategy and implementation plan for VA to Congress on September 28, 2015, as promised.

OI&T is committed to protecting all Veteran information and VA data and limiting access to only those with the proper authority. This commitment requires us to think enterprise-wide about security holistically. We have dual responsibility to store and protect Veterans records, and our strategy addresses both privacy and security. We designed our strategy to counter the spectrum of threat profiles through a multi-layered, in-depth defense model enabled through five strategic goals.

- **Protecting Veteran Information and VA Data:** We are strongly committed to protecting data. Our data security approach emphasizes in-depth defense, with multiple layers of protection around all Veteran and VA data.
- **Defending VA's Cyberspace Ecosystem:** Providing secure and resilient VA information systems technology, business applications, publically accessible platforms, and shared data networks is central to VA's ability to defend VA's cyberspace ecosystem. Addressing technology needs and operations that require protection, rapid response protocols, and efficient restoration techniques is core to effective defense.
- **Protecting VA Infrastructure and Assets:** Protecting VA infrastructure requires going beyond the VA-owned and VA-operated technology and systems within VA facilities to include the boundary environments that provide potential access and entry into VA by cyber adversaries.
- **Enabling Effective Operations:** Operating effectively within the cyber sphere requires improving governance and organizational alignment at enterprise, operational, and tactical levels (points of service interactions). This requires VA to integrate its cyberspace and security capabilities and outcomes within larger governance, business operation, and technology architecture frameworks.
- **Recruiting and Retaining a Talented Cybersecurity Workforce:** Strong cybersecurity requires building a workforce with talent in cybersecurity disciplines to implement and maintain the right processes, procedures, and tools.

VA's Enterprise Cybersecurity Strategy is a major step forward in VA's commitment to safeguarding Veteran information and VA data within a complex environment. The strategy establishes an ambitious yet carefully crafted approach to cybersecurity and privacy protections that enable VA to execute its mission of providing quality health care, benefits, and services to Veterans, while delivering on our promise to keep Veteran information and VA data safe and secure.

We are working to close key actions in response to oversight recommendations, thus, eliminating our label as a material weakness in VA. In addition to publishing our strategy, we have:

- Established eight domains to address findings from Office of Inspector General FISMA audits and improve cybersecurity posture;
- Fully funded Continuous Readiness in Information Security Program (CRISP) efforts;
- Named a new Chief Information Security Officer; and
- Conducted penetration testing with multiple parties.

As part of CRISP, our Enterprise Cybersecurity Strategy Team has created a detailed Material Weakness Plan and is on track to eliminate our material weaknesses by the end of 2017.

In addition, we have a large legacy issue that we need to address. VA is increasing our spending on security to \$370 million, fully funding and fully resourcing our security capability. In addition, we are investing over \$50 million to create a data-management backbone.

Goals for 2016 and beyond

This year, we are aiming to achieve key milestones on the path to creating a world-class IT organization that improves the support to business partners and Veterans. To do this we will:

- Add five new functions to the IT organization.
- Create the account management office.
- Develop portfolios for all Administrations and Staff Offices.
- Finish at least 50 percent of projects on time and on budget. (i.e., best practice for the industry is 55-58 percent)
- Tie performance goals for all SES to strategy goals.
- Begin to close all current cybersecurity weaknesses— all by 2017
- Develop a holistic Veteran data management strategy.
- Implement a quality and compliance office.
- Deploy a transformational vendor management strategy.
- Ensure implementation of key initiatives to improve access to care.
- Strengthen Electronic Health Record Strategy.

- Establish one authoritative source for Veteran contact information, military service history, and Veteran status.
- Finalize the Congressionally mandated DoD-VA Interoperability requirements.

Conclusion

Mr. Chairman, this concludes my testimony. I thank you again for the opportunity to discuss our new IT strategy with you today. Throughout this transformation, our number one priority has and will be always the Veteran— ensuring a safe and secure environment for their information and improving their experience is our goal. I am pleased to answer any questions you or the Subcommittee may have.



Department of Veterans Affairs

Senior Executive Biography

LaVerne H. Council, MBA, DBA

**Assistant Secretary for Information and Technology
and Chief Information Officer,
Office of Information and Technology**

Ms. LaVerne H. Council joined the Department of Veterans Affairs in July 2015 as the Assistant Secretary for Information and Technology (OI&T) and Chief Information Officer. In this role, Ms. Council oversees the day-to-day activities of VA's \$4 billion IT budget and over 8,000 IT employees to ensure that VA has the IT tools and services needed to support our Nation's Veterans.



Prior to joining VA, Ms. Council served as CEO of Council Advisory Services, LLC and Chair of the National Board of Trustees for the March of Dimes. In December 2011, she retired from Johnson & Johnson after serving as Corporate Vice President and Chief Information Officer for Johnson & Johnson's global Information Technology group. In this capacity, she was responsible for managing information technology and related systems for the \$61.6B Johnson & Johnson worldwide enterprise. She was a Member of the Corporate Global Operating Committee and her organization included more than 250 operating companies with over 4,000 information technology employees and 7,000 contractors.

Ms. Council is a proven visionary senior executive with global experience in the development and execution of cutting-edge information technology and supply chain strategies in the healthcare/life sciences, consumer products and telecommunications/hi-tech industries. In 2011, Ms. Council received the Alumni Business Achievement Award from Ernst & Young. Business Trends Quarterly named her as one of the top four CIOs in America in 2010. The New Jersey Technology Council inducted her into their CIO Hall of Fame in 2009, and the Global CIO Executive Summit named her a Top 10 Leader and Change Agent in 2009 and a Top 10 Leader and Innovator in 2008. CAREER CHRONOLOGY:

2015 – Present	Assistant Secretary, Information and Technology, Department of Veterans Affairs
2012 – 2015	CEO, Council Advisory Services, LLC
2011 – Present	Chairperson of the National Board of Trustees, March of Dimes Foundation
2006 – 2011	Corporate Vice President and Chief Information Officer, Johnson & Johnson
2000 – 2006	Global Vice President for Information Technology, Global Business Solutions and Development Services, Dell, Inc.

Ms. Council was also a partner with Ernst and Young and led the company's Global Supply Chain Strategy practice. She also held leadership positions focusing on infrastructure engineering, networking, security and enterprise application interfaces.

EDUCATION:

2010	Doctorate of Business Administration, Drexel University, Philadelphia, PA
1986	Master of Business Administration, Operations Management from Illinois State University, St. Normal, IL
1983	Bachelor of Science in Business, Western Illinois University, Macomb,