STATEMENT OF
MS. LAVERNE COUNCIL
ASSISTANT SECRETARY FOR INFORMATION TECHNOLOGY AND
CHIEF INFORMATION OFFICER
DEPARTMENT OF VETERANS AFFAIRS
BEFORE THE
HOUSE COMMITTEE ON VETERANS' AFFAIRS
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS (O&I)
AND THE
HOUSE OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON COMMITTEE ON INFORMATION TECHNOLOGY

October 27, 2015

Introduction

Chairmen Hurd and Coffman, Ranking Members Kelly and Kuster, and Members of the Committees, thank you for the opportunity to appear before you today to discuss the state of the Office of Information and Technology (OI&T) at the Department of Veterans' Affairs (VA). I am accompanied today by Brian Burns, Deputy Director of the Interagency Program Office. I am proud to be a part of the VA team, where we have the greatest mission in government: to care for our Nation's Veterans. I believe we can – and must – do better to deliver excellent healthcare and benefits to our Veterans through World-Class Information Technology (IT), and I am delighted to discuss our new OI&T Strategy with you today.

VA OI&T Is At a Critical Inflection Point

VA's Office of Information and Technology is at a critical inflection point. Persistent internal challenges exist in delivering IT services, and external pressures are compelling OI&T to change and adapt. With MyVA, we have the opportunity to become the authors of our own story, MyVA gives our team the chance to make a difference in the Veterans' experience.

Our aspiration is to transform OI&T into a world-class organization. IT is an enabler of each of VA's disparate lines of business, including the largest integrated healthcare

system in the United States; a benefits processing organization equivalent to a medium-size insurance company; one of the largest integrated memorial and cemetery organization in the country; a court system; and many other components.

In addition, we are rolling out a new strategic plan for OI&T. The new strategy has a new mission, vision, guiding principles, and strategic goals and I am proud to share these with you today. Our mission is to collaborate with our business partners to create the best experience for all Veterans. Our vision is to become a world-class organization that that provides 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. We will establish a strong technical foundation that ensures alignment with VA's mission, data visibility and accessibility, data interoperability, infrastructure interoperability, information security, and enterprise services. Finally, we have to execute these goals through a prioritized set of strategic initiatives across our Now, Near, and Future time horizons: in order to stabilize and streamline core processes, to eliminate the material weaknesses, and to institutionalize a new set of capabilities to drive improved outcomes.

This transformation will be different. We will measure success, ensure accountability, invest in the capabilities of OI&T employees, and collaborate across the VA to build trust. Over the next six months, we will complete a number of quick wins – initiatives that will be initiated to drive maximum impact for business partners and Veterans in the short term – in order to drive immediate positive change and begin the transformation into a world-class IT organization that provides the best possible service to its business partners and Veterans.

A comprehensive review of the organizational assessments, strategic plans, and customer and employee feedback reveal persistent challenges within OI&T:

- *Customer focus*: insufficient collaboration between OI&T and customers and lack of service-level agreements
- *Standardization and quality*: aging IT infrastructure combined with low data quality and lack of integration
- *Leadership and organization*: leadership communication not effective, and key functions duplicated across OI&T and VA
- *Innovation*: lack of methods and processes to enable innovation for our customers
- *Governance*: OI&T not measuring what matters, leading to ineffective governance and inability to continuously improve
- *Project management*: current process burdened with excessive overhead; lacks consistency and accountability
- *Budgeting*: process disconnected from total lifecycle costs
- *Acquisition*: acquisition process not aligned across VA and OI&T
- *Workforce development*: insufficient talent management

In addition, significant factors increase pressure on OI&T to change and adapt. VA faces *changing Veteran demographics* as the aging Veteran population seeks out and uses benefits (e.g., long-term care) at significantly higher rates. OI&T has *shifting business partner needs*, with new and increasing diversity of customer needs, types of applications, and complexity of the IT support required (e.g., Telehealth) driving the overall demand on OI&T. *Rising public expectations* have become a factor due to increasing public discourse around willingness and trust in government to deliver health services for Veterans. *Growing cyber threats* are a significant factor with the persistent risk of cyber attacks, combined with the continuing digitization of health care, and the increasing exposure, vulnerability, and potential consequences of a data breach. The *next generation IT delivery models* increase pressure through the evolution of external IT delivery models and with the increasing adoption of services and more commercial-style techniques (e.g., learning by doing). A movement toward *consumerization of IT* is

an added pressure factor as the technology landscape, fueled by an emphasis on real-time, mobile-first, hyper-targeted digital experiences, increasingly demands the same experiences in the workplace. Finally, the rapidly growing number of sensors and actuators connected by networks to computing systems, known as the *Internet of Things*, drives complexity on how to manage our environments, blurring the lines between IT and the "things".

The Opportunity Is Now

We have established four key OI&T objectives that align with myVA objectives. First, we will implement our OI&T strategy through three phases: Now, Near, and Future. These phases encompass a durable, long-term strategy built to transcend 36 months. Second, we will adopt a customer-centric mindset throughout the end-state design process, including collaborative engagement with all key stakeholders. Third, we will institutionalize a "buy-first" strategy that leverages existing commercial solutions first before building internally. Finally, will incorporate best practices from the public and private sector to spur agility, efficiency, effectiveness, and innovation in service delivery.

The opportunity is now, because we have the key components for success. We have executive-level support from the Secretary and Deputy Secretary, and the CIO role at VA is empowered with unique flexibility. I've been impressed to find that we have a hard working, mission-oriented staff that cares deeply about creating a better experience for the Veteran. Through Congressional action, we have a centralized IT and sufficient resources. Finally, we have the ability to deliver for our business partners when they need us the most.

We Will Transform

The strategic goals and framework are aligned with the key priorities from all VA strategic plans. Under our first theme of *stabilizing and streamlining core processes and platforms*, our plan calls for the establishment of an Enterprise Program Management Office, as well as a data management organization. We will also redesign our enterprise processes. Our theme of *eliminating the material weaknesses* focuses on addressing material weaknesses identified by the Federal Information Security Modernization Act (FISMA) and (FISCAM), implementing our enterprise cybersecurity plan, and establishing a quality and compliance organization. Our final theme of *institutionalizing a new set of capabilities to drive improved outcomes* calls for establishing account management, transforming our Service Delivery Organization, and launching a new vendor management function.

This transformation will be different because ensuring successful execution of this plan requires a new approach. We will deliver *Quick wins* and we will implement *rigorous performance management*, and will enforce it by measuring success through specific metrics tied to Veteran outcomes. We will *institutionalize a "buy-first" strategy*, leveraging existing commercial solutions first before building internal capabilities. We will invigorate *employee engagement and accountability*, creating performance goals that cascade throughout the organization, giving each employee a role in making our strategy a reality. We will improve *leadership and skills training*, addressing capability gaps across the workforce, including developing leaders that can see the big picture, improve their performance, and drive relentless change. And, we will improve *cross-VA collaboration*, building trusted relationships across all levels, including transparent communication across the VA to improve Veterans and employees' experience.

EPMO: Interoperability and Electronic Health Record Modernization

Finally, I would like to focus specifically on two of our quick wins, the establishment of an Enterprise Program Management Office (EPMO) and the creation of the Enterprise Cybersecurity Strategy. The EPMO is especially relevant to the committee's interest in VA's interoperability and health record modernization efforts by improving execution and outcomes for Veterans and VA. The IT EPMO will initially host our biggest IT programs for better project portfolio and resource tracking, and will improve communication around these programs and projects. Upon establishment of the EPMO, we will integrate four of our biggest programs into the EPMO: VistA Evolution, Interoperability, the Veterans Benefits Management System (VBMS), and Medical Appointment Scheduling System (MASS).

The IT EPMO will ensure alignment of program portfolios to strategic objectives and provide visibility and governance into the programs. It will also allow for better analysis of and reporting on programs, projects, resources, and timelines to optimize for the best mix of each. This will help ensure the overall health of portfolios through reporting and analysis of portfolio performance metrics. For enterprise initiatives, the IT EPMO will help program and project teams to better develop execution plans, monitor progress, and report status. It will enable partnerships with IT architects for enterprise collaboration, and will serve as a program/project resource for delivery of enterprise and cross-functional programs. Doing so will help identify Shared Services Enterprise Programs and will help plan resource requirements with portfolios and architecture. Finally, with an IT EPMO, communication will improve through better management of internal and external communication and employee engagement. It will enable the coordination of enterprise communications through the development of comprehensive, enterprise communication strategies to drive consistency of messaging.

We have begun to identify the right leaders for the EPMO, as well as the senior leaders who will lead the initial programs. Specifically for VistA Evolution, I have tasked the program leads to create a clear and persuasive business case that clearly explains

measurable outcomes to Veterans. They will deliver this case next week to myself and Dr. David Shulkin, the Under Secretary for Health. Dr. Shulkin and I, the co-Executive Sponsors for the program, will determine the next steps in this program based on the case that is presented.

Regarding interoperability, VA and DoD share millions of health records between our systems today. Having a Veteran's complete health history, from both DoD and VA, as well as community providers, is critical to providing seamless, high quality access to care and benefits. In the third quarter of FY 2015, the Departments maintained data for 7.4 million unique correlated patients and unique DoD patients registered in the Master Veterans Index. Over the past year, VA has also seen rapid growth in utilization of the Joint Legacy Viewer, or 'JLV'. JLV is a read-only web based health record viewer that allows both VA and DoD to see a Veteran or Service member's complete health history from both Departments, integrated on a single screen. As of last week, VA had over 19,000 authorized JLV users, up from just a few hundred this time last year, when JLV became available at all VA medical centers. Currently, we are making JLV available to nearly 1,000 new users each month, with about 25 percent in VBA and 75 percent in VHA.

However, sharing data is only the first step in interoperability. Shared data needs to be used to provide better health care and benefits services to Veterans. I am happy to report this is happening, and we are learning a lot from our users in the field which is helping us iteratively refine and improve our new products. A VA dermatologist in Seattle estimates JLV saves him about a minute in completing a tele-dermatology consultation. He sometimes completes over 50 such consults a day, so a minute saved on each really adds up. One of our primary care providers has said JLV is particularly helpful for finding DoD immunizations for her patients, and is using JLV regularly in her primary care clinic. In VBA, users are telling us JLV is very helpful for evaluating cases with missing records, and that it helps them find a lot more information for Guard and Reserve Veterans. We are also working on community facing pilots for JLV, as part of our strategy to improve interoperability and data exchange with providers outside the

VA and DoD. One pilot program is exploring use of JLV at CVS Minute Clinics in the Palo Alto, California area. In this pilot, Veterans would have the option of being referred to a Minute Clinic for minor illnesses, and could authorize VA to provide health information to the Minute Clinic via the Joint Legacy Viewer.

All of the great capabilities we have developed in JLV with our DoD partners will be carried forward into our new enterprise Health Management Platform, or 'eHMP'. We have recently brought eHMP into production in the Austin Information Technology Center, and in Hampton, Virginia, and we will have many more sites in production over the next several months. The next release of eHMP is a modern, read-write web application and data services platform, which will ultimately replace the current Computerized Patient Record System used today by all VA providers at the point of care. eHMP will natively federate all available health information for Veterans, from all sources in DoD, VA, and community providers from whom we have data. This is a tremendous step forward for VA health information technology, and will allow us to more effectively support Veteran centric, team based, quality driven care.

Another critical component for advancing interoperability is the Veterans Health Information Exchange program (VLER Health), which provides information exchange with our Community Partners through eHealth Exchange and Direct. VLER Health focuses on: 1) engaging Veterans to sign authorization forms to exchange their health care data; 2) onboarding Community Partners to build a national network; 3) developing stable and scalable technical systems that provide secure conduits for Veterans' health information exchange; and 4) accelerating VA clinical adoption. In FY2015 the VLER Health program grew significantly, with a current total of 59 partners and a 300 percent increase in use of the program by VHA clinicians. Obtaining Veteran Authorization forms continues to be a significant barrier for our external partners, as Opt-In consent is required before VHA can release information with community health care providers for treatment of shared patients. A Legislative Proposal was submitted earlier this year for Congress to consider amending Title 38 United States Code Section 7332 to permit VA to disclose health information protected by the statute to non-VA health care providers

for treatment of shared patients without the written authorization of the patient. This amendment would permit VA to move to an Opt-Out consent model for health information exchange consistent with most national partners and providers, and permit VA to share this health information with CHOICE providers treating Veterans more efficiently and timely.

In all of our interoperability efforts, VA is working closely with the DoD/VA Interagency Program Office and the Office of the National Coordinator for Health Information Technology to ensure correct national standard codes are used for describing our health information data. We are also beginning to discuss additional standards needed for information reconciliation, for domains such as allergies and medications.

Enterprise Cybersecurity Strategy

One of my first acts as CIO was the formation of the Enterprise Cybersecurity Strategy Team (ECST). 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. Meeting this commitment requires a comprehensive strategic approach that spans VA and the cyberspace ecosystem in which Veterans, VA, and VA's partners operate. By its very nature, the Internet is an open system facilitating the free flow and exchange of information, ideas, and commerce, embodying some of the very principles upon which this Nation was founded. The very same qualities are accompanied by a growing number of vulnerabilities and risks threatening our Nation's security, stability, and prosperity.

VA, its core constituents, and external partners are all subject to a wide variety of these threats. Given the high degree of connectivity, mutual interdependence, and reliance on integrated open platform technology, meeting cybersecurity challenges requires dedicated strategic attention. VA's Enterprise Cybersecurity Strategy is focused on building a comprehensive cybersecurity capability supportive of VA's overall

transformation effort to secure the execution of the MyVA mission as it modernizes VA technical culture, processes and capabilities.

The strategy answers several critical questions:

- What are the right things to do to achieve our cybersecurity mission and vision?
- How do we know we are doing the right things?
- Are we making decisions and investments that deliver our cybersecurity strategy?
- Are we aligning our resources to deliver the strategy?
- Are we achieving intended outcomes?

The strategy is predicated on protecting and countering the spectrum of threat profiles through a multi-layered defense in depth model enabled through five strategic goals.

1. *Protecting Veteran Information and VA Data:* Ensuring secure technology and data systems to protect all VA data is insufficient in and of itself.
2. *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.
3. *Protecting VA Infrastructure and Assets:* Protecting VA infrastructure requires going beyond the technology and systems wholly owned and operated by VA within its facilities to include the boundary environments that provide potential access and entry into VA by cyber adversaries.
4. *Enabling Effective Operations:* Operating effectively within the cybersphere 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.

5. *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 healthcare, benefits, and services to Veterans while delivering on our promise to keep Veteran information and VA data safe and secure.

Conclusion

Chairmen and Ranking Members, thank you again for the opportunity to discuss our new strategy for IT at VA with you today. Throughout this transformation, our number one priority is always the Veteran – ensuring a safe and secure environment for their information, and approaching the security of Veteran data from the Veteran's point of view in concert with Secretary McDonald's MyVA strategy. I am committed to seeing this strategy through and leaving behind an improved OI&T when my term is over. I am happy to take your questions at this time.