VA CYBERSECURITY AND IT OVERSIGHT

HEARING

BEFORE THE

SUBCOMMITTEE ON
INFORMATION TECHNOLOGY

OF THE

COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

MARCH 16, 2016

Serial No. 114–133

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PUBLISHING OFFICE

25–503 PDF WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JASON CHAFFETZ, Utah, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
JIM JORDAN, Ohio
TIM WALBERG, Michigan
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
CYNTHIA M. LUMMIS, Wyoming
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
RON DESANTIS, Florida
MICK, MULVANEY, South Carolina
KEN BUCK, Colorado
MARK WALKER, North Carolina
ROD BLUM, Iowa
JODY B. HICE, Georgia
STEVE RUSSELL, Oklahoma
EARL L. "BUDDY" CARTER, Georgia
GLENN GROTHMAN, Wisconsin
WILL HURD, Texas
GARY J. PALMER, Alabama

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MATT CARTWRIGHT, Pennsylvania
TAMMY DUCKWORTH, Illinois
ROBIN L. KELLY, Illinois
BRENDA L. LAWRENCE, Michigan
TED LIEU, California
BONNIE WATSON COLEMAN, New Jersey
STACEY E. PLASKETT, Virgin Islands
MARK DESAULNIER, California
BRENDAN F. BOYLE, Pennsylvania
PETER WELCH, Vermont
MICHELLE LUJAN GRISHAM, New Mexico

JENNIFER HEMINGWAY, *Staff Director*
TROY STOCK, *IT Subcommittee Staff Director*
MICHAEL FLYNN, *Counsel*
SHARON CASEY, *Deputy Chief Clerk*
DAVID RAPALLO, *Minority Staff Director*

SUBCOMMITTEE ON INFORMATION TECHNOLOGY

WILL HURD, Texas, *Chairman*

BLAKE FARENTHOLD, Texas, *Vice Chair*
MARK WALKER, North Carolina
ROD BLUM, Iowa
PAUL A. GOSAR, Arizona

ROBIN L. KELLY, Illinois, *Ranking Member*
GERALD E. CONNOLLY, Virginia
TAMMY DUCKWORTH, Illinois
TED LIEU, California

CONTENTS

VA CYBERSECURITY AND IT OVERSIGHT

Wednesday, March 16, 2016

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INFORMATION TECHNOLOGY,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, D.C.

The subcommittee met, pursuant to call, at 2:00 p.m., in Room 2247, Rayburn House Office Building, Hon. William Hurd [chairman of the subcommittee] presiding.

Present: Representatives Hurd, Farenthold, Kelly, and Connolly.

Also Present: Representative Moulton.

Mr. HURD. The Subcommittee on Information Technology will come to order. Without objection, the chair is authorized to declare a recess at any time.

Last June, in the first hearing on the data breach of the Office of Personnel Management, I told agencies that we would be watching to make sure they are taking their cybersecurity obligations seriously. We discussed how CIOs, CISOs, and agency heads need to take a hard look at their IG audits and GAO reports, and make sure they address the findings to make sure their cyber posture is meeting FISMA standards. The same is true when addressing the federal IT acquisition reforms. That is why this committee, in a bipartisan fashion, developed a scorecard to grade agencies on their implementation of FITARA.

This committee will continue to hold agency heads responsible for the state of their agency information technology and cybersecurity posture, but much of this work starts in the office of the CIO. We are here today to continue that work, and nearly no other department is of such importance to get right as the second largest Federal agency whose mission it is to care for our Nation's veterans. We cannot afford and should not allow IT lapses to occur.

While we are focusing on the technical details today, I hope each of us will also take time to recognize that there are real-world consequences and impacts of these decisions, and that they fall upon those who have already given so much for their country. We cannot forget that.

Ms. Council, I am pleased to have you here today. I know this is your sixth hearing, I think, in the last 10 days, so I appreciate it. I think it is because you are so charming and you know what you are doing, so it is great to have you here.

Truthfully, I am very encouraged. I am encouraged that you have a strategy in place to eliminate material weaknesses, material weaknesses that, in some cases, go back 17 years.

The VA exceeded the OMB's target on 30-day the cybersecurity sprint and expanded strong authentication practices to 100 percent of its privileged users and 80 percent of its unprivileged users. This was demonstrated progress in the area of cybersecurity and a positive indicator that the VA is making progress in this area. But concerns remain.

The goal you and your chief information security officer have set to eliminate the material weaknesses is by the end of 2017, 2 years to solve in some cases fairly basic cybersecurity best practices. We are talking about predictive scanning for vulnerabilities, implementing risk assessment, monitoring tools, and security training. Two years is too long, and I think we can do better.

The VA received an overall grade on the committee's FITARA scorecard of a C. The agency received Fs in savings relating to data center consolidation and IT portfolio review. Again, I must highlight this is self-reported data.

We will talk about that and the VA's plan to implement FITARA further.

The modernization of the VA's legacy technology is a real concern that is affecting millions of veterans.

Ms. Council, a few weeks ago, you testified before the House Appropriations Committee that you "want to take a step back from the existing modernization plan of VistA. You cited changes in circumstances and issues such as women's health, the Internet of Things, and Care in the Community as instigating factors in taking a pause on the VistA Evolution plan developed in 2014.

While I certainly appreciate big thinking, especially in government IT, I have to ask whether or not this is another example of the VA taking a U-turn on substantial IT investment. We have been down this road before with the effort to make electronic health records of the DOD and VA interoperable.

Is VistA going to end up in a multiyear investment that never delivers the functionality that the VA's health care providers need? The meaningful exchange of health care data has been delayed for far too long.

While the DOD and VA seem to have made progress recently with the Joint Legacy Viewer. I want to reiterate once again that the JLV is not true interoperability.

The missed deadlines, cost overruns, and failures to deliver on expectations leave me with serious doubts about whether these two departments are able to work together toward effective, real-time sharing of veterans' health data.

Turning to the issue of patient scheduling, what will a pause of VistA Evolution mean for the medical appointment scheduling system? Here again is a problem that needs an IT solution that has suffered repeated setbacks.

This is not a new problem. The scheduling component of VistA dates back to 1984. With veterans coming home from the wars in Iraq and Afghanistan, this is a system that needs to be upgraded immediately. Fifty-thousand schedulers made 80 million appointments in fiscal year 2011 alone—80 million.

The VA has recently put in place a 5-year contract to develop a new medical appointment scheduling system at the cost of $624 million. I have to ask the questions: Could this have been done

cheaper with commercial off-the-shelf technology? Will the latest attempt work? Will this contract fix the scheduling problems at the VA?

I have said it time and again, the problems the agencies face in IT and cybersecurity are not in the availability or accessibility of technology. The tools already exist. The challenge the Federal agencies face, and we have seen at OPM and the Department of Education, is having the leaders in place, leaders who have vision and a commitment to staying at their agency to see the vision through.

And, Ms. Council, I am excited because I think you are the right person for the job.

I thank the panel for attending today's hearing, and I look forward to today's discussion.

Now it is my pleasure and honor to recognize the gentlelady from Illinois, my friend and ranking member of the subcommittee, Ms. Kelly, for her opening remarks.

Ms. KELLY. Thank you, Mr. Chairman.

Information technology is critical to improving the service and performance of the Federal Government, especially the Department of Veterans Affairs, one of the largest integrated health care systems in the United States, serving millions of veterans and families.

Today's hearing provides the VA an opportunity to demonstrate their commitment to improving the delivery of health care and benefits to our veterans, while safeguarding the veteran information and VA data that exists within its environment.

This committee plays an important oversight role that can increase transparency and accountability of agency efforts to implement important legislation such as the FITARA and FISMA.

In response to various internal challenges and external pressures, VA rolled out a new strategy to transform the Office of Information and Technology into a world-class IT organization that supports the delivery of excellent health care and benefits to veterans. Transforming an IT organization of 8,000 employees with a budget of more than $4 billion is no simple task.

The VA chief information officer, Ms. Council, joined VA in July 2015, inheriting an IT environment with thousands of outstanding security risks and failed or mismanaged IT projects. However, Ms. Council's written testimony to this subcommittee in October stated, and I quote, "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."

I look forward to hearing more on the progress at VA and recognizing the Office of Information and Technology to better manage the IT portfolio and enhance CIO authority and accountability as required by the FITARA.

Given the recent breaches in both the public and private sector, we are all aware of the evolving nature of threats facing information systems. It is important that we ensure that the VA responds to these threats with efforts to fully address information security weaknesses and enhance its information security posture. These efforts to improve VA operations and information security are essential to regaining the trust and confidence of the American public that the VA is taking care of our Nation's vets.

Thank you, Mr. Chairman.

Mr. HURD. Thank you.

Now I will hold the record open for 5 legislative days for any members who would like to submit a written statement.

Mr. HURD. We will now recognize our panel of witnesses. I am pleased to welcome the Honorable LaVerne Council, Assistant Secretary for Information and Technology and chief information officer at the Office of Information and Technology of the U.S. Department of Veterans Affairs.

Ms. Council is accompanied by Brian Burns, Deputy Assistant Secretary for Information Security at the Office of Information and Technology at the U.S. Department of Veterans Affairs, whose expertise may be needed during questioning.

Next, I would like to welcome Brent Arronte, Deputy Assistant Inspector General for Audits and Evaluations with the Office of Inspector General at the U.S. Department of Veterans Affairs. Mr. Arronte is also accompanied by Mr. Michael Bowman, director of the Information Technology and Security Audits Division at the Office of the Inspector General, whose expertise may be needed during questioning as well.

Welcome to you all. Pursuant to committee rules, all witnesses will be sworn in before they testify. We will also swear in Mr. Burns and Mr. Bowman.

So please rise and raise your right hands.

Do you solemnly swear or affirm the testimony you are about to give will be the truth, the whole truth, and nothing but the truth?

Thank you. Please be seated.

Let the record reflect that the witnesses answered in the affirmative.

In order to allow time for discussion, please limit your testimony to 5 minutes. Your entire written statement will be made part of the record.

Ms. Council, we will start with you, and you are recognized for 5 minutes.

WITNESS STATEMENTS

STATEMENT OF LAVERNE COUNCIL

Ms. COUNCIL. Thank you, Chairman Hurd, Ranking Member Kelly, and distinguished subcommittee members. Thank you for the opportunity to discuss the progress we are making towards serving our Nation's veterans.

In October, I shared with you our plan to transform the Office of Information and Technology, or OI&T, into a world-class organization by implementing a new enterprise strategy. Our mission is

to collaborate with our business partners to create the best experience for all veterans.

We are becoming a principles-based organization, one centered on transparency, accountability, innovation, and teamwork.

Our team is transforming. We are infusing a new perspectives and skills by hiring new talent. We have added five senior leaders and will add an additional 11 in the next 90 days. This team will carry the torch for relentless execution.

When our veterans interact with VA, they are making the choice to entrust us with their personal information. The delivery of VA's enterprise cybersecurity strategy in September 2015 was the first reinforcement of our commitment to safeguard their information with tools, technology, and the people of the highest caliber.

We have made significant progress in improving our cybersecurity posture. For the first time, our security efforts are fully funded and resourced at $370 million in fiscal years 2016 and 2017. This investment will make the implementation of our plan a reality.

OI&T can no longer be considered a material weakness for VA. We are addressing all key FISMA findings. By the end of 2016, we will close 30 percent of the IG's recommendations, and we will close 100 percent by the end of 2017.

We have reduced elevated privileges by 95 percent, and we will technically enforce personal identity verification, or PIV, to achieve our 80 percent goal by September.

But the highest level of security does not rest with IT alone. We are providing comprehensive education to ensure that all VA employees remain vigilant. We have updated our national rules of behavior and our annual security training, and we are emphasizing continuous engagement with our employees.

Information security poses constant challenges, and it is only through continuous reinforcement that our employees can support us in this battle.

We have achieved several significant goals in implementation of our Enterprise Program Management Office, or EPMO. The EPMO began operating on February 1 and is now our control tower, mapping out an agile path for all IT efforts. We replaced the Program Management Accountability System, or PMAS, with our new Veteran-focused Integration Progress, or VIP. VIP reduced our overhead obligation by 88 percent.

Our most important projects, including VistA Evolution or VistA 4, the Enterprise Health Management Platform, VBMS, and our interoperability processes are already transitioned to VIP.

For the first time, OI&T will have an integrated 18-month portfolio, a single change and a single release calendar. We will also include a 90-day post-release warranty on all efforts to ensure the highest levels of performance.

Access to accurate veteran information is one of our core responsibilities. We will jointly be certifying interoperability with DOD, as mandated by the 2014 NDAA, within the next month and ahead of the 2016 deadline. We are outpacing our projection for our interoperability tool, the Joint Legacy Viewer, which has over 44,000 users and grows by over 3,000 weekly.

But we must do more. We are evaluating our electronic health record modernization plans to ensure we have the right strategy in place for the next 25 years, well beyond what will be achieved in 2018 by VistA 4.

This is not about the software. This is about supporting the veteran anytime, anywhere. We must strive for continuous innovation, not just for NEHR, but for a digital health platform. We owe it to our veterans to evaluate their needs and meet each veteran where she is.

I am proud of our recent accomplishments. But transformation requires a relentless focus on outcome, outcomes that matter, outcomes that support the veterans who have supported us.

Mr. Chairman, members of the subcommittee, thank you again for the opportunity to discuss our progress with you. I am happy to take your questions at this time.

[Prepared statement of Ms. Council follows:]

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*.

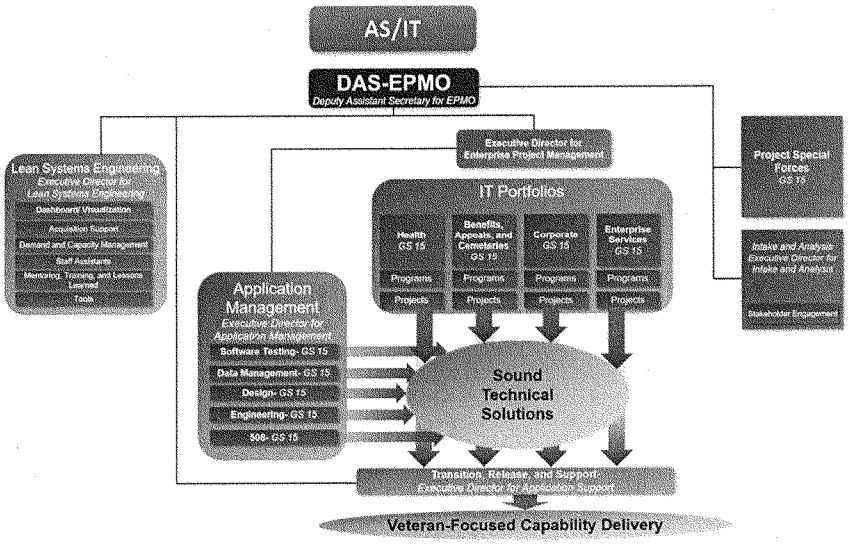

Fig. 1 – EPMO Organizational Chart

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.

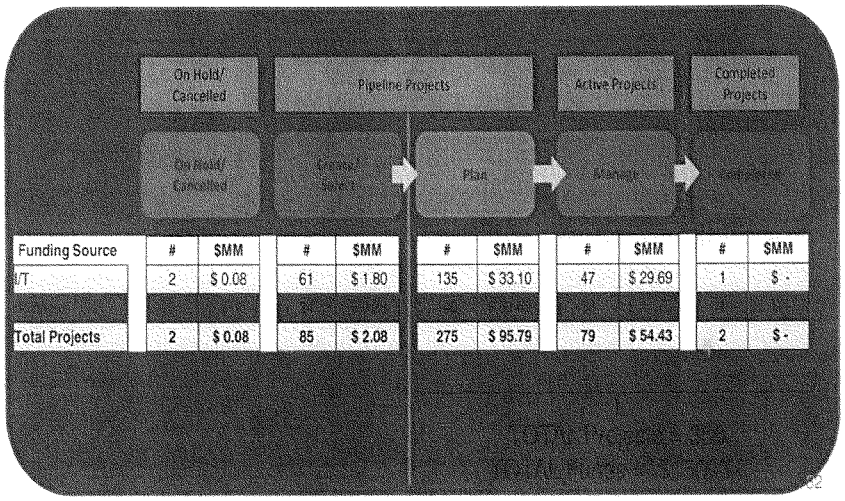

Fig. 2 – Sample Project Framework Pipeline

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. EPMO 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	VIP
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

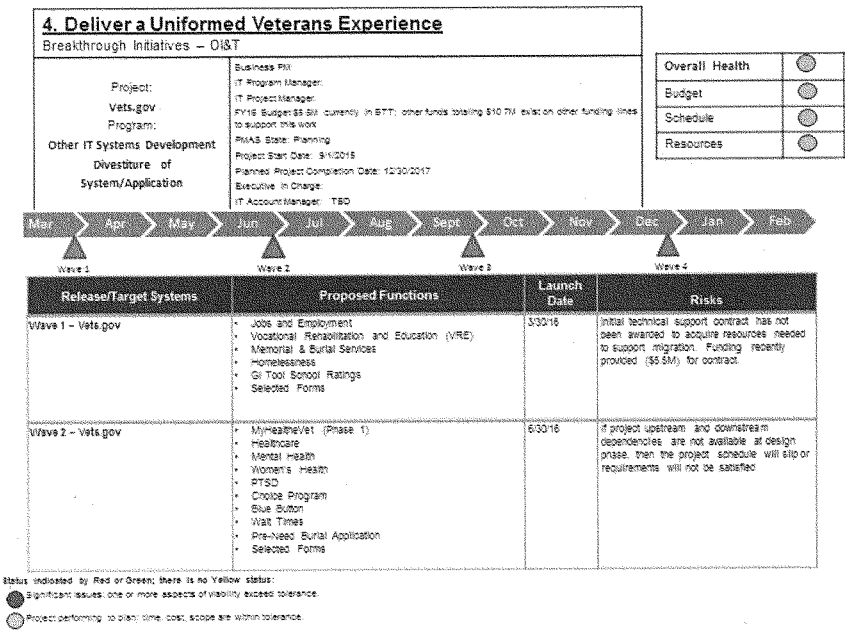

Fig. 4 – OI&T Breakthrough Initiatives

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.

Mr. HURD. Thank you, Ms. Council.

Now I would like to recognize Mr. Arronte for 5 minutes.

STATEMENT OF BRENT ARRONTE

Mr. ARRONTE. Mr. Chairman and members of the subcommittee, thank you for the opportunity to discuss the Office of Inspector General's work regarding the VA's management of information technology and information security.

As previously indicated, I am accompanied by Mr. Michael Bowman, OIG's director of Information Technology and Security Audit Division.

VA continues to face challenges in developing IT systems it needs to support its current goals and overall mission. For 16 consecutive years, information security has been reported as a material weakness in VA's consolidated financial statement audit. Our audits have shown that IT system development and management at VA is a longstanding, high-risk challenge.

Despite some advances, our reports indicate VA IT programs are still often susceptible to cost overruns, schedule slippages, and performance problems.

Over the past 3 years, the OIG has made 69 recommendations to improve IT systems management and security. As of February 2016, 57 of those recommendations remain open. Of those 57, 17 are repeat recommendations and 13 are modified repeat recommendations.

For fiscal year 2016, the VA estimates a total IT investment of about $4.1 billion to fund information system security, system development initiatives, and systems operation and maintenance. If not properly planned and managed, these to IT investments can become costly, risky, and counterproductive.

In March 2012, the VA instituted the Continuous Readiness and Information Security Program, also known as CRISP. The purpose of CRISP is to ensure continuous, year-round monitoring and to establish a team responsible for resolving IT material weaknesses. While VA implemented some standardized information security controls, these improvements require time to be fully implemented and to show if they are effective.

Our limited review indicates the CRISP initiative has not been fully effective in addressing systemic weaknesses or eliminating material weaknesses found in VA's information security program for fiscal year 2015.

Examples of some of these weaknesses are financial management systems using outdated technology, password standards not consistently implemented, and systems not securely configured to mitigate known and unknown information security vulnerabilities.

In April 2015, our administrative investigative staff found that certain OI&T employees failed to follow VA information security policy and contract security requirements. Specifically, OI&T staff improperly approved VA contractors to work remotely and access VA's network from foreign countries such as China and India.

We identified that one contractor used his personally owned laptop to access VA's network from China. This contractor had administrative rights as well. Upon completion of his work, he left

the laptop in China. As of this date, the laptop has not been recovered.

We also found that other VA contractor employees improperly connected to the VA's network from other foreign locations. We determined VA information security officials and the former executive in charge for OI&T failed to quickly and effectively respond to determine if there was a compromise as a result of VA contractors accessing VA networks internationally.

VA is also challenged in developing IT systems needed to support mission goals. Recent OIG reports disclose that some progress has been made in timely deploying system functionality because of the agile system development method. Despite these advances, VA continues to struggle with cost overruns and performance shortfalls.

VA's mechanism for overseeing IT program management has improved but has not been fully effective in controlling these IT investments. Our work has demonstrated that VA continues to struggle with its IT investments.

Some improvements in information security have become evident with the inception of CRISP. However, more work remains to be done, and VA needs to remain focused on addressing OIG recommendations in the security and development of IT systems.

Until a proven process is in place to ensure controls across the enterprise, the IT material weakness may stand and VA's mission-critical systems and sensitive veterans data may remain at risk of attack or compromise.

Mr. Chairman, this concludes my statement. We would be happy to answer any questions you or other members of the subcommittee may have.

[Prepared statement of Mr. Arronte follows:]

BRENT ARRONTE
DEPUTY ASSISTANT INSPECTOR GENERAL FOR
AUDITS AND EVALUATIONS
OFFICE OF INSPECTOR GENERAL
DEPARTMENT OF VETERANS AFFAIRS
BEFORE THE
SUBCOMMITTEE ON INFORMATION TECHNOLOGYCOMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES
HEARING ON
"VA INFORMATION TECHNOLOGY AND CYBERSECURITY OVERSIGHT"
MARCH 16, 2016

Mr. Chairman and Members of the Subcommittee, thank you for the opportunity to discuss the Office of Inspector General's (OIG) work regarding the VA's management of information technology and information security. Our statement will focus on the effectiveness of VA's information security program and progress made and challenges VA continues to face in developing the systems it needs to care out is missions and program. We base our conclusions on OIG reports on VA's information security program and our oversight of information technology (IT) systems development activities. I am accompanied by Mr. Michael Bowman, Director, OIG's Information Technology and Security Audits Division.

BACKGROUND

IT systems and networks are critical to VA in carrying out its mission of providing medical care and a range of benefits and services to veterans. Ensuring the secure operation of these systems and networks is essential, given the wide availability of hacking tools on the internet and the advances in the effectiveness of attack technology. Lacking proper safeguards, the systems and networks are vulnerable to intrusions by groups seeking to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other systems. VA has previously reported security incidents in which sensitive information, including personally identifiable information, has been lost or stolen, potentially exposing millions of veterans and their families to the loss of privacy, identity theft, and other financial crimes.

For fiscal year (FY) 2016, VA estimates a total IT investment of about $4.1 billion to fund information system security, system development initiatives, and system operations and maintenance. To the extent that VA does not properly plan and manage these IT investments, they can become costly, risky, and counterproductive. In addition, although IT investments may be managed by the Office of Information Technology (OIT), it is imperative to include input from VA business owners and other stakeholders throughout the incremental system development process.

Our audits in recent years also show that IT system development at VA is a longstanding high-risk challenge, susceptible to cost overruns, schedule slippages, performance problems, and in some cases, complete project failures. Also in 2015, the

Government Accountability Office identified VA's management of IT acquisitions and operations as "high risk" and in their report they cited some significant failed VA IT investment projects totaling approximately $735 million.[1] In addition, the Government Accountability Office identified Security of Federal Information Systems as "high risk" and stated that Cybersecurity incidents to systems supporting the federal government and national critical infrastructures have significantly increased over the past eight years.

INFORMATION SECURITY

In November 2015, for the16th consecutive year, the OIG's independent contractors that perform the annual audit of VA's consolidated financial statements have identified IT security controls as a material weakness. This work supports our requirements to perform annual Federal Information Security Modernization Act (FISMA) assessments. FISMA requires agencies to develop, document, and implement agency-wide information security risk management programs and prepare annual reports. FISMA also requires that each year, the OIG assess the extent to which VA complies with FISMA's information security requirements, information security standards developed by the National Institute of Standards and Technology (NIST), and the annual reporting requirements from the Office of Management and Budget.

In March 2012, VA instituted the Continuous Readiness in Information Security Program (CRISP) to ensure continuous monitoring year-round and establish a team responsible for resolving the IT material weakness. In our report, *Federal Information Security Management Act Audit for Fiscal Year 2015* (March 15, 2016), we discussed more focused VA efforts to implement standardized information security controls across the enterprise. For example, we reported that:

- VA had updated its policy which establishes a foundation for VA's comprehensive information security and privacy program and its practices based on applicable NIST Special Publications.
- VA's Chief Information Officer formed an Enterprise Cybersecurity Strategy team that was charged with delivering an enterprise cybersecurity strategic plan designed to help achieve greater transparency and accountability while securing veteran information.
- VA continued to implement an IT Governance, Risk, and Compliance tool to improve the process for assessing, authorizing, and monitoring the security posture of the agency.
- VA improved implementation of security awareness training for all employees and individuals with outdated background investigations had been reduced.
- Data center web application security had been improved.

[1] The Department of Veterans Affairs' (VA) Financial and Logistics Integrated Technology Enterprise program, which was intended to be delivered by 2014 at a total estimated cost of $609 million, but was terminated in October 2011 due to challenges in managing the program and the VA Scheduling Replacement Project, which was terminated in September 2009 after spending an estimated $127 million over 9 years.

However, these improvements require time to be fully implemented and show evidence of their effectiveness. Despite progress made, the CRISP initiative was not fully effective in addressing systemic weaknesses and eliminating the material weakness. We continue to see repeat information security deficiencies in type and risk level to our reported findings in prior years and an overall inconsistent implementation of the security program. Communication between the CRISP team and VA site managers also needs improvement. Our FY 2015 FISMA audit report discussed control deficiencies in four key areas: configuration management controls, access controls, security management, and contingency planning controls.

Configuration Management Controls are designed to ensure critical systems have appropriate security baseline controls and up-to-date vulnerability patches implemented. However, we found:

- Systems including key databases supporting various applications were not timely patched or securely configured to mitigate known and unknown information security vulnerabilities.
- The financial management system uses outdated technology that hinders mitigation of certain vulnerabilities.
- VA needs to strengthen its methodologies for monitoring medical devices and ensuring they are properly segregated from other networks.
- Baseline configurations, including implementation of the Federal Desktop Core Configuration, were not consistently implemented to mitigate significant system security risks and vulnerabilities across the facilities.
- Change control policy and procedures for authorizing, testing, and approval of system changes were not consistently implemented for the networks and mission critical system hardware and software changes.
- Several VA organizations shared the same local network at some medical centers and data centers; however, the systems were not under the common control of the local site. Some organizational systems often had critical or high-level vulnerabilities that weakened the overall security posture of the VA sites.
- Formal processes were lacking to prevent installation of or remove unauthorized application software on VA systems.

Access Controls are designed to ensure that password standards are consistently implemented across the enterprise and that user accounts are monitored to enforce minimal access privileges necessary for legitimate purposes and to eliminate conflicting roles. Our FISMA assessment revealed that:

- Password standards were not consistently implemented and enforced across multiple VA systems, including the network domain, databases, and mission critical applications. In addition, multi-factor authentication for remote access had not been fully implemented across the agency.
- Inconsistent reviews of networks and application user access resulted in numerous generic, system, and inactive user accounts that were not removed or deactivated from the system, and users with access rights that were not appropriate.

- Proper completion of user access requests was not consistently performed to eliminate conflicting roles and enforce principles of least system privilege.
- Monitoring of access was lacking in the production environment for individuals with elevated application privileges for a major application.
- Identification, notification, and remediation of security incidents were not consistently implemented to ensure incidents were resolved timely. In addition, network security event logs were not consistently maintained or reviewed across all facilities.

Security Management is designed to ensure that system security controls are effectively monitored on an ongoing basis and system security risks are effectively remediated through corrective action plans or compensating controls. We reported that:

- Security management documentation, including the risk assessments and System Security Plans, were outdated and did not accurately reflect the current system environment or Federal standards.
- Background reinvestigations were not performed timely or tracked effectively. In addition, personnel were not receiving the proper level of investigation for the sensitivity levels of their positions.
- Plans of Action and Milestones (POA&Ms) were not completed by their milestone dates and were not updated to reflect changes to milestones. POA&M closures were not supported with adequate documentation. VA had approximately 9,500 open POA&Ms in FY 2015 compared with 9,000 in FY 2014. POA&Ms identify which actions must be taken to remediate system security risks and improve VA's overall information security posture.
- VA did not effectively manage and monitor its systems hosted at a cloud service provider.

Contingency Planning Controls ensure that mission-critical systems and business processes can be restored in the event of a disaster or emergency. However, we determined that:

- Backup tapes were not encrypted prior to being sent to offsite storage at selected facilities and data centers.
- Contingency plans did not reflect the current operating environment. Specifically, contingency plans had not been updated to reflect changes in system boundaries, roles and responsibilities, and lessons learned from testing contingency plans.

Further, we continued to identify significant technical weaknesses in databases, servers, and network devices that support transmitting sensitive information among VA Medical Centers, Data Centers, and VA Central Office. Within our annual FISMA report, we discuss security deficiencies where control activities were not appropriately designed or operating effectively. Inconsistent application of vendor patches to address such weaknesses jeopardized the data integrity and confidentiality of VA's financial and sensitive information.

Moving forward, VA needs to complete implementation of an enterprise-wide information security program and improve its monitoring process to ensure controls are operating as intended at all facilities. The dispersed locations, the continued reorganization of VA business units, and the diversity in applications adversely affected facilities and management's ability to consistently remediate IT security deficiencies agency-wide. For example, VA's dispersed financial system architecture resulted in a lack of common system security controls and inconsistent maintenance of IT mission-critical systems. Consequently, VA continues to be challenged by a lack of consistent enforcement of established policies and procedures throughout its geographically dispersed portfolio of legacy applications and newly implemented systems. In addition, VA lacked an effective and consistent corrective action process for identifying, coordinating, correcting, and monitoring known internal security vulnerabilities on databases, web applications, and networks infrastructures. Effective communication between VA management and the individual field offices is critically needed to notify the appropriate personnel of identified security deficiencies so that they can timely implement corrective actions.

Our FY 2015 FISMA report included 31 recommendations to the Assistant Secretary for Information and Technology for improving VA's information security program. The report also highlighted 4 unresolved recommendations from prior years' assessments for a total of 35 outstanding recommendations. Overall, we recommended that VA:

- Address security-related issues that contributed to the IT material weakness reported in the FY 2015 audit of the Department's consolidated financial statements.
- Remediate high-risk system security issues within its POA&Ms.
- Establish effective processes for evaluating information security controls via continuous monitoring and vulnerability assessments.
- Implement effective automated mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and Web application servers.
- Institute procedures to oversee contractor management of cloud-based systems, ensure OIG access to those systems, and ensure information security controls are adequate to protect sensitive VA systems and data.
- Conduct periodic reviews to minimize access by system users with incompatible roles, permissions in excess of required functional responsibilities, and excessive or unauthorized accounts.

We are evaluating VA's progress during our current work on the FY 2016 FISMA audit and acknowledge increased VA efforts to improve information security. This fall, upon completion of our FY 2016 FISMA testing and related work at 24 of sites nationwide, including VA's four major data centers, we will make a determination as to whether VA's improvement efforts are successful in eliminating the IT material weakness.

OTHER INFORMATION TECHNOLOGY CONCERNS AT VA

VA faces the added challenge of overcoming several information security concerns not highlighted in previous years, such as the reorganization of OI&T's regional structure and new leadership of the CRISP program without institutional knowledge as a result of turnover of senior leadership. Where appropriate, we are pursuing these issues as a part of our ongoing FISMA audit work. Otherwise, we are conducting separate reviews or pursuing other means to address the issues noted below.

Limited Reporting of Security Incidents to the OIG

VA continues to experience security breaches of its enterprise as a result of employee and contractor actions, malware, or "focused operations actors" activity. However, the reporting of these incidents to OIG has been relatively low and limited. In accordance with FISMA, VA must provide the OIG with timely notifications of network intrusions and system compromises so we can properly execute our oversight function.

The following are examples of security incidents not properly reported to the OIG:

- Since December 2010, we have noted six incidents involving compromises of VA contractor owned computers or user credentials resulting in unauthorized access into VA networks. The two most recent contractor computer compromises occurred in February 2015 and May 2015; however only the latter security incident was ever reported to the OIG.
- Since November 2014, the Network Security and Operations Center (NSOC) has identified two incidents of keystroke logging software data on devices with one containing logged Veterans Health Information Systems and Technology Architecture (VistA) user credentials. Despite Federal requirements, neither of these incidents were reported to the OIG. Keystroke loggers are typically used to capture user credentials so malicious users can gain unauthorized access onto computer systems.
- In June 2015, the NSOC identified network traffic associated with certain software used to enable anonymous communication across the Internet and to conceal users' identity and location. The resulting analysis identified a VA domain administrator using a computer and security device that prevented the NSOC from evaluating the machine for compliance with VA security requirements. The NSOC initially reported this issue to the OIG as "cracked" Corel Draw software. However, the NSOC did not disclose any information to us regarding the use of anonymizing software or the security implications of using a security device to prevent compliance checks.
- In light of recent Office of Personnel Management data breach, the NSOC has evaluated enterprise activity for "Indicators of Compromise" and identified 7 potentially compromised hosts. While VA's Forensic Investigation Service is currently analyzing these computers for security compromises, the OIG was never notified of these security issues. We proactively discovered this information when reviewing VA's Remedy System.

As a result, we are not satisfied with the inconsistent reporting of security incidents to the OIG.

Veterans Health Information Systems and Technology Architecture

We have evaluated certain key controls within VistA as part of our FISMA audit. Specifically, we have reviewed VistA controls supporting financial transactions that are reported in VA's consolidated financial statements each year. However, we have not evaluated VistA's on-going evolution and its interoperability with Department of Defense's electronic health record (EHR) application. Recently, we reported that certain audit controls within VistA were not enabled, which limited our oversight work in order to determine whether any malicious manipulation of scheduling data or unauthorized access to VistA records occurred at several VA Medical Centers noted below. Additionally, we discovered during a recent investigation at the Washington DC VA Medical Center that VistA email was purged without sufficient backups, resulting in an unknown quantity of email that is unrecoverable.

In February 2015, the OIG's Office of Healthcare Inspections conducted a review of the care a patient received at the Atlanta VA Medical Center, in Decatur, Georgia, and evaluated an improper disclosure of protected information outside VA.[2] We confirmed that an individual with access to a patient's VistA EHR improperly disclosed protected health information outside VA. The patient's record was designated as "non-sensitive" at the time of the disclosure. As a result of this designation, the Veterans Health Administration (VHA) lacked the ability to audit access to VistA "non-sensitive" records. More importantly, managers do not have the necessary tools to identify wrongdoers and therefore cannot consistently enforce some rules and statutes. To date, OIG investigators were unable to determine who accessed the patient's EHR or who was responsible for the improper disclosure. VA's Interim Under Secretary for Health concurred with our recommendations and agreed to evaluate the feasibility of enabling system audit logging for all patient records.

In February 2015, the OIG's Office of Healthcare Inspections conducted another inspection to assess the merit of allegations of poor and delayed care of a patient in the Urgent Care Clinic at the Tomah VA Medical Center in Tomah, Wisconsin.[3] One specific allegation stated that unauthorized parties accessed or disseminated a patient's electronic health record information inappropriately. The complainant provided several Internet news article "comments" that were potentially indicative of sensitive VistA EHR information having been accessed and used in an inappropriate manner. After reviewing these comments, we did not identify any protected information that could only have been obtained from the patient's VistA EHR or other VA privacy protected documents. However, we found that it was possible that the patient's VistA EHR was accessed inappropriately since the record was designated as "non-sensitive" and was not monitored. When a record is designated as "non-sensitive," an electronic audit trail is not created when the EHR is accessed. The patient's record was not designated "Sensitive" until February 25, 2015. VA's Interim Under Secretary for Health concurred with our recommendations and agreed to evaluate the feasibility of enabling system audit logging for all patient records.

---

[2] *Evaluation of a Patient Care and Disclosure of Protected Information, Atlanta VA Medical Center, Decatur Georgia* (June 23, 2015).
[3] *Care of an Urgent Care Clinic Patient, Tomah VA Medical Center, Tomah Wisconsin* (June 18, 2015).

In August 2014, we reported that certain audit controls within VistA were not enabled, which hurt our ability to determine whether any malicious manipulation of the VistA scheduling data occurred at the Phoenix VA Health Care System, in Phoenix, Arizona.[4] Consequently, we requested that OIT leadership enable all audit trails within the scheduling system. We also requested that OIT discontinue deleting VistA accounts for former employees and instead place these accounts in a disabled state so that we can evaluate system use and scheduling data as part of our review. OIT complied with these requests. The OIG is committed to performing additional scrutiny of the functionality and data integrity of this system as part of ongoing and future reviews.

Improper Access to the VA Network by VA Contractors from Foreign Countries

In April 2015, an OIG administrative investigation found that certain OIT employees failed to follow VA information security policy and contract security requirements when they improperly approved VA contractor employees to work remotely and access VA's network from China and India, respectively.[5] We noted that one contractor accessed VA's network from China using personally-owned equipment that he took to and left in China, and the other accessed VA's network from India using personally-owned equipment that he took with him to India and then brought back to the United States. Further, we found that a VA employee and other VA contractor employees improperly connected to VA's network from foreign locations. We further noted that VA information security officials and the Executive in Charge for OIT failed to quickly and effectively respond to determine if there was a compromise as a result of VA contractor employees accessing VA's network internationally.

Improper Use of Web-based Collaboration Technology

In August 2015, we reported that VA employees improperly used Yammer.com, a Web-based collaboration technology that was not approved or monitored as required by VA policy.[6] Further, we found the application had vulnerable security features, recurring website malfunctions, and users were engaged in a misuse of time and resources. Although One VA Technical Reference Model approved the installation of Yammer's "Notifier" desktop application, the use of the Yammer social network was not approved for VA employee use. Furthermore, we noted that the Internet based application was used and showcased by the Executive in Charge of Information Technology and Chief Information Officer, for an open chat forum, as well as in a CIO Message reminding employees to comply with VA Directive 6515 when using Yammer. This direction gave the false impression that VA had approved employees' use of Yammer.com. As of July 14, 2015, Yammer.com reflected there were 24,864 VA email addresses registered with active members and another 25,252 VA email addresses registered which were not yet activated.

---

[4] *Review of Alleged Patient Deaths, Patient Wait Times, and Scheduling Practices at the Phoenix VA Health Care System* (August 26, 2014).
[5] *Administrative Investigation – Improper Access to the VA Network by VA Contractors from Foreign Countries Office of Information and Technology Austin, TX (April 13, 2015).*
[6] *Administrative Investigation – Improper Use of Web-based Collaboration Technology Office of Information and Technology* (August 17, 2015).

We also found that Yammer users violated VA policy when they downloaded and shared files, videos, and images, risking malware or viruses spreading quickly from the site. We further noted that Yammer regularly spammed and excessively emailed users, as well as VA employees who had no interest in joining the site. In addition, users were unable to remove the "Online Now" instant messaging feature, resulting in every user violating VA policy simply by logging onto the site. We found numerous user posts that were non-VA related, unprofessional, or had disparaging content that reflected a broad misuse of time and resources. Moreover, the continuous data streams, instant messaging, video, audio, large attachment files, and other uploaded non-VA content to the site can cause disruption of service and degrade the performance of VA's network. OIT's lack of control over the Yammer website has made VA vulnerable to users uploading personally identifiable information, protected health information, or VA sensitive information, of which any current or former employee active on the site would have access.

Data Sharing Violations at the Palo Alto VA Medical Facility

In October 2014, we received an allegation that the VA Palo Alto Health Care System (PAHCS), in Palo Alto, California, Chief of Informatics entered into an illegal agreement with Kyron, a health technology company, to allow data sharing of sensitive VA patient information. This allegation involved veterans' personally identifiable information, protected health information, and other sensitive information that was transmitted outside of VA's firewall. The complainant also alleged Kyron personnel received access to VA patient information through VA systems and networks without appropriate background investigations.

In September 2015, we did not substantiate the allegations that the Chief of Informatics formed an illegal agreement with Kyron or that sensitive patient information was transmitted outside of VA's firewall. However, we reported that Kyron personnel received access to VA patient information without appropriate background investigations.[7] Further, the Information Security Officers (ISOs) failed to execute their required responsibilities in accordance with VA Handbook 6500, Information Security Program, by not providing PAHCS management and staff guidance on information security matters. The lack of coordination between facility program proponents and ISOs resulted in Kyron having access to VA information systems without appropriate background investigations and Kyron's software being used on a VA server without formal approval. VA's Assistant Secretary for Information and Technology concurred with our findings and recommendations and provided an acceptable corrective action plan.

Cloud Computing

In February 2013, we communicated concerns to VA regarding its intent to migrate its e-mail systems to a cloud service provider. Specifically, VA had moved 15,000 email user accounts to a cloud-based system as part of a pilot study and planned to migrate the remaining 600,000 email user accounts to the virtual cloud environment thereafter. As

[7] *Review of Alleged Data Sharing Violations at VA's Palo Alto Health Care System* (September 28, 2015).

a result, all VA email messages were planned to be hosted on a contractor-owned and operated system.

Upon OIG review of the underlying contract, we noted the contract did not require the cloud service provider to provide OIG access to VA systems and data stored at the contractor facilities. Consequently, the OIG would not have legal access to VA systems and data needed for investigative and oversight purposes. Further, the contract terms would potentially compromise our efforts to ensure that annual FISMA requirements are met. Additionally, the contract lacked requirements for the cloud service provider to segregate VA sensitive data from other customer data, potentially impeding OIG investigations and creating new information security weaknesses involving VA electronic data. VA planned to adopt a policy to delete cloud-hosted emails greater than 90 days old in an effort to save costs with the cloud-based contract. Email is integral to the manner in which VA conducts day-to-day business. As such, retention of emails is critical to support VA work, OIG investigations and oversight reviews, and to defend VA actions in the administrative and judicial appellate systems.

In April 2013, the OIG issued a memorandum to the then-Deputy Secretary requesting that VA cease further contracting to put VA data in the cloud until all mission requirements of the OIG, VA General Counsel, and other VA administrations were met. Further, we requested that VA users not delete any email from any VA system until record management systems are established providing a minimum retention period of 7 years. We requested that all cloud-based systems be assessed at a "high" impact risk level to ensure that VA sensitive data are physically and logically segregated from other customer data hosted on the same virtual computer platforms. After several discussions with VA senior leadership, the then-Deputy Secretary directed that OIT terminate the email cloud-based contract because of concerns regarding retention of non-record emails raised primarily by the OIG, as well as by General Counsel.

Enterprise Archiving System

The OIG has communicated major concerns to VA's senior leadership regarding retrieval of Enterprise Archive System emails prior to June 2013. Currently, VA stores archived emails on a "Digital Safe" device which VA uses to support email collections pursuant to our oversight work. In June 2015, we were notified that VA's "Digital Safe" was not working properly and all email content prior to June 2013 was not readily available to support OIG investigations or VA legal discovery requests. OIT originally stated that the "Digital Safe" problem would be resolved in September 2015, but the targeted resolution date has moved to May 2016.

While VA has been able to provide email prior to June 2013, due to the "Digital Safe" not working properly, the process is extremely labor intensive and time consuming, resulting at times in delays that impair the OIG's and VA's Office of General Counsel's ability to satisfy its oversight and legal responsibilities, respectively. The lack of a viable solution to provide timely "Digital Safe" data negatively impacts the OIG's internal operations by delaying receipt of archived emails associated with multiple OIG investigations and inspections. The lack of timely access to this data also adversely

affects both the VA's and the OIG's obligation to comply with legal discovery requirements from the Department of Justice, other administrative bodies as well as requests for information from Congress. Accordingly, we are concerned that VA lacks sufficient resources, processes and data to support operational transparency and accountability.

Personally Identifiable Information Transmission Over Unsecure Internet Connections

In March 2013, we reported that VA was transmitting sensitive data, including personally identifiable information and internal network routing information, over an unencrypted telecommunications carrier network.[8] VA disclosed that personnel typically transfer unencrypted sensitive data, such as electronic health records and internal internet protocol addresses, among certain VA Medical Centers and Community-Based Outpatient Clinics using an unencrypted telecommunications carrier network. OIT acknowledged this practice and formally accepted the security risk of potentially losing or misusing the sensitive information exchanged.

These risks continue to exist across the VA enterprise. Despite concurring with our report findings and recommendations, VA has not fully implemented the technical configuration controls needed to ensure encryption of sensitive data in accordance with VA and Federal information security requirements. Without controls to encrypt the sensitive VA data transmitted, veterans' information may be vulnerable to interception and misuse by malicious users as it traverses unencrypted telecommunications carrier networks. Further, malicious users could obtain VA router information to identify and disrupt mission-critical systems essential to providing health care services to veterans.

INFORMATION TECHNOLOGY SYSTEMS DEVELOPMENT

VA remains challenged in developing the IT systems it needs to support VA's mission goals. Recent OIG reports disclose that some progress has been made in timely deploying system functionality because of the Agile system development methodology. This methodology allows subject matter experts to validate requirements and functionality in increments of 6 months or fewer, while technology is developed and updated to meet user needs. Despite these advances, VA continues to struggle with cost overruns and performance shortfalls in its efforts to develop several major mission-critical systems. VA's mechanism for overseeing IT program management has improved but has not been fully effective in controlling these IT investments. Inadequate IT human capital management plays a notable role in these system development outcomes.

Veterans Benefits Management System

In February 2013, we issued a report, *Review of VBA's Transition to a Paperless Claims Processing Environment,* evaluating whether VA had performed sufficient testing of the Veterans Benefits Management System (VBMS) and assessing whether VA was positioned to meet its goal of eliminating the disability claims backlog and increasing the accuracy rate of processing claims to 98 percent by 2015.[9]

---

[8] *Review of Alleged Transmission of Sensitive VA Data Over Internet Connections* (March 6, 2013).
[9] *Review of Transition to a Paperless Claim Processing Environment* (February 4, 2013).

As of September 2012, VBMS was still in the early stages of development. We found that due to the use of VA's Agile incremental development approach, the system had not been fully developed to the extent that its capability to process claims from initial application through review, rating, award, to benefits delivery could be sufficiently tested. While we did not evaluate the quality of system testing, we determined the partial VBMS capability deployed as of that date had experienced system performance issues. At the time of that audit work, VA senior officials stated they had taken recent actions to improve in the areas identified. However, given the incremental system development approach used and the complexity of the automation initiative, we concluded VA would continue to face challenges in meeting its goal of eliminating the backlog of disability claims processing by 2015. Because the system was in an early stage of development, we could not examine whether VBMS was improving VBA's ability to process claims with 98 percent accuracy. The then-Under Secretary for Benefits and the then-Assistant Secretary for Information and Technology concurred with our report recommendations that VA establish a plan with milestones for resolving system issues and develop a detailed approach to scanning and digitizing claims so that transformation efforts do not adversely affect claims processing and add to the claims backlog.

In September 2015, we issued a follow-up review to determine whether VA has improved its schedule, cost, and performance in VBMS development to better position VA to meet its claims processing accuracy and backlog elimination goals.[10] We reported that VA deployed certain planned VBMS functionality to all VA Regional Offices in 2013, largely due to the incremental Agile development approach. With the deployments, VA has expanded automated claims processing functionality, supported improved data exchange, and standardized business practices that VA reports have helped reduce the claims processing backlog. However, total estimated VBMS costs increased significantly from about $579 million initially in September 2009 to about $1.3 billion in January 2015. Further, we found VBMS still did not fully provide the capability to process claims from initial application through review, rating, award, to benefits delivery. The system continues to experience performance issues, including service disruptions and slowness. VBMS cost overruns and performance shortfalls were chiefly due to unplanned changes in system and business requirements and a lack of performance metrics. Until these issues are addressed, VA will remain unable to ensure effective return on its VBMS investment. Further, until a fully functioning system is in place, VA will be challenged to meet its 98 percent claims processing accuracy and backlog elimination goals. VA's Executive in Charge for the Office of Information and Technology, in conjunction with Veterans Benefits Administration (VBA), generally agreed with our findings and recommendations.

We are currently reviewing allegations related to VBA failing to integrate suitable audit logs into VBMS. We will report out on this work in late Spring.

---

[10] *Follow-up Review of the Veterans Benefits Management System* (September 14, 2015)

Pharmacy Reengineering

In December 2013, we reported on OIT's management of the Pharmacy Reengineering (PRE) project.[11] OIT restarted PRE in October 2009 under the Project Management Accountability System (PMAS). PRE is critically needed to help address patient safety issues associated with adverse drug events. Although some progress had been made, OIT had not been effective in keeping the PRE project on target in terms of schedule and cost, as well as the functionality delivered. Deployed PRE functionality had improved patient safety. However, project managers have struggled to deploy PRE increments in a timely manner. Project managers were also unable to provide reliable costs at the increment level. OIT restarted PRE at a time when PMAS had not evolved sufficiently to provide the oversight needed to ensure project success.

As such, PRE management was challenged in keeping the project on track. Consequently, OIT was at an increased risk of not completing PRE on time and within budget. Moreover, the future of Pharmacy Reengineering was uncertain due to potential plans to transfer funding and remaining development to the Integrated Electronic Health Record (iEHR) project in FY 2014. Stronger accountability over cost, schedule, and scope for the remaining development is needed prior to such a transfer so that iEHR is not compromised by the same challenges.

VA's Executive in Charge and Chief Information Officer agreed with our recommendations to ensure all of the time used, including the time on the initial operating capability phase, to complete each remaining PRE increment is reported and monitored; ensure adequate oversight and controls, including the planning guidance, staffing, and cost and schedule tracking needed to deliver functionality on time and within budget; and establish a plan for future funding of PRE until iEHR is decided. OIT now requires paused projects to pass a review that serves as a critical checkpoint before they can advance to an active development state. OIT implemented controls to ensure all projects maintain adequate staffing. Further, OIT has provided adequate funding for PRE to move forward with continued development.

Program Management Accountability System

VA launched PMAS in June 2009 to improve its ability to deliver successful IT projects. At the request of VA's Chief Information Officer, we conducted an audit in 2011 to evaluate the effectiveness of PMAS planning and implementation. We reported that a great deal of work remains before PMAS can be considered completely established and fully operational.[12] For example, OIT created and instituted the PMAS concept without a roadmap, adequate leadership, and staff to effectively implement and manage the new methodology. If such foundational elements are not fully implemented, the discipline and accountability needed for effective management and oversight of IT development projects will not be instilled. VA's Chief Information Officer concurred with our findings and recommendation and provided an acceptable corrective action plan.

[11] *Audit of VA's Pharmacy Reengineering Software Development Project* (December 23, 2013).
[12] *Audit of the Project Management Accountability System Implementation* (August 29, 2011).

In 2014, we performed a follow-up audit to evaluate whether OIT took effective actions to address recommendations that we made in our prior audit report on PMAS. In our report, we noted that OIT had taken steps to improve PMAS.[13] For instance, OIT had defined PMAS roles and responsibilities, developed guidance for re-planning paused projects, and established controls to ensure essential staff is assigned to manage the projects. However, at the time of that report, OIT needed to take additional actions to improve IT project accountability and oversight and the PMAS Business Office still lacked sufficient leadership and staff. We reported that the PMAS Dashboard retained an incomplete audit trail of baseline data and project managers continued to struggle with capturing and reporting costs. These issues occurred because OIT did not appropriately address our prior report recommendations. Project managers also did not report costs for enhancements to existing systems on the PMAS Dashboard due to unclear PMAS guidance. As a result, OIT and therefore VA leaders lack reasonable assurance these IT investment projects are delivering functionality on time and within budget. We also identified potentially $6.4 million in cost savings OIT could achieve by hiring Federal employees to replace contract employees currently augmenting PMAS Business Office staff. VA's Executive in Charge concurred with most of our recommendations and provided acceptable corrective action plans.

CONCLUSION

Our work has demonstrated that VA continues to struggle with its IT investments and securing IT systems. Some improvements in information security management have become evident with the inception of CRISP. However, more work remains to be done and VA needs to remain focused on addressing OIG recommendations in the security and development of IT systems. Until a proven process is in place to ensure control across the enterprise, the IT material weakness may stand and VA's mission-critical systems and sensitive veterans' data may remain at risk of attack or compromise. IT shortfalls mean not only exposure of millions of veterans to potential loss of privacy, identity theft, and other financial crimes, they also would constitute poor financial stewardship and counterproductive investments of taxpayer dollars.

Mr. Chairman, this concludes my statement. We would be happy to answer any questions you or other members of the Subcommittee may have.

[13] *Follow-Up Audit of the Information Technology Project Management Accountability System* (January 22, 2015).

Mr. HURD. Thank you, sir.

I now would like to recognize the gentleman from Texas, Mr. Farenthold, for 5 minutes for questioning.

Mr. FARENTHOLD. Thank you very much, Mr. Chairman.

Ms. Council, you talked a little bit about upgrading your medical records system. If your electronic medical records system was in the private sector, would it be compliant with all the laws applicable to the private sector, HIPAA laws and all the other new requirements under the Affordable Care Act?

Ms. COUNCIL. Not all the new laws. That is one of the reasons that we are developing a new strategy that we need to go forward with for the next 25 years. So, no, it would not, not all the ACA.

Mr. FARENTHOLD. And it is also my understanding that a lot of both your hardware and software is grossly out of date. I was down in the Rio Grande Valley and the Secretary of the VA mentioned to the group some of the financial systems are actually running computer language called COBOL, which was actually around probably before I was born, and I am in my 50s.

Is it a problem to maintain and update this code and find employees to do that?

Ms. COUNCIL. The current state of the financial systems is that we are looking for a shared platform with our financial organization. They are looking at Treasury as a Federal opportunity to engage a partner.

So you are right, the systems are older. As a person in her 50s as well, and COBOL being a language that I know quite well, it is old, and we do need to upgrade.

Mr. FARENTHOLD. What sort of effect is this out-of-date software having on delivering service to our veterans and making sure that the physicians who provide service either under the voucher system or Veterans Choice are paid in a timely fashion?

Ms. COUNCIL. I think you have touched on the main issue as to why we are looking at a digital health platform, sir. The reality is when you are on old platforms, old hardware, old software, you cannot take advantage of the new opportunities to share data, as well as upgrade our information with those providers and pay them quicker.

That is really our focus, to ensure that we are prepared for the future.

Mr. FARENTHOLD. And it is not just the software that is out-of-date or your custom software. It is even some of the stuff you buy off-the-shelf. It is my understanding you all have not yet completely migrated off Windows XP, which is no longer supported by Microsoft.

Ms. COUNCIL. There are 834 custom applications within the VA. The most customs that I have ever seen in my career. We also do have XP in the environment, much of that leveraged by medical cyber and medical equipment.

As part of our enterprise cybersecurity strategy, we have put in processes to eliminate and drive out that lifecycle problem.

Mr. FARENTHOLD. Are we also looking in the VA at moving away from the extraordinary number of custom systems? There is a lot of off-the-shelf stuff that you ought to be able to adopt. Is that not a reasonable question?

Ms. COUNCIL. It is a very reasonable question, sir. There are five new functions we are adding as part of the strategy. One of those new functions is strategic sourcing, which is all about putting us in a situation where we buy versus build, so that we look for off-the-shelf software that can meet our needs first. We validate that there is not something that is already built that could meet our needs, and then we make those calls based on what best fits the process.

Mr. FARENTHOLD. I can understand that there is some legacy stuff that was designed to run on Windows XP and may not run on other stuff. Our research shows that you all are still on Exchange Server 2003 that had an end-of-life-support cycle in 2014.

Do you think the outdated software that is not getting current security patches might be a cybersecurity opening or vulnerability?

Ms. COUNCIL. We actually use the same assessing process that the IG uses and patch aggressively against each of those issues, as well as taking those software out.

One of the big opportunities that we have and we are deploying within the next month a contract to start moving much of this to the cloud using Email as a Service, moving much of that storage out into the cloud in a secure manner working with the IG. It gives us an opportunity to eliminate some of the hardware issues that we have, but also put ourselves in a new place, as far as transformation.

Mr. FARENTHOLD. I want to direct this final question to anybody on the panel that would like to answer. Is there anything that Congress is not doing that it should be doing to help you through this IT crisis and get you to where you can better deliver services to our veterans? Obviously, the answer is to give us more money, but maybe we can do a little better than just that.

Ms. COUNCIL. I always say this because it still continues to be the issue. When you are hiring for information technology, the kinds of architects we need, the kinds of security people we need, we are competing against private resources. And it takes a while to get into the Federal Government, and the requirements are not those that those same resources and highly valued resources would face in private industry.

We need those resources, and even as we get access and opportunities to meet those people to talk with them, we take a long time to get them in the door. So any help that can be given there will be the most important help you can give us.

Mr. FARENTHOLD. And if you can get us some specifics on that, we want you to be able to compete with Google for the good people.

Ms. COUNCIL. I appreciate it. I have three or four resumes I will get to you.

Mr. FARENTHOLD. Did anyone else want to answer that?

All right. I will yield back the remainder of my time.

Mr. HURD. Thank you, Mr. Farenthold.

Now I would like to recognize the ranking member for her 5 minutes of questioning.

Ms. KELLY. Thank you again.

Ms. Council, as chief information officer, you oversee the activities of VA's $4 billion IT budget and over 8,000 IT employees in support of the VA's mission. Information technology at the VA in-

cludes a wide variety of tools and systems that support VA's mission to care for our Nation's vets. Your testimony highlights the creation of the Enterprise Program Management Office, which will host VA's biggest IT programs and help VA meet FITARA requirements.

When will of the EPMO be fully functional? And how will you ensure the office achieves its desired results?

Ms. COUNCIL. The EPMO actually came on February 1, which means that we stood the team up. We are building the program management. We are talking to union about some of the new roles. All those things around people should be fully completed by April 1, as far as the union.

But that means we have already started working. We have hired in, out of the Department of Commerce, the head for all of our pillars. As I mentioned, our top four projects are all under VIP. There are 12 core projects in which we are validating every step of the process.

By the end of September, every single project will be working under VIP, which will move us to true agile development. The PMAS process, which people knew about, really was one that focused on waterfall. This will be true agile, and it will reduce our overhead by over 88 percent and increase our ability to deliver by only requiring seven core necessary documents and available to operate at the beginning of the process.

All these things should move us into a situation where we deliver every quarter versus every 6 months.

Ms. KELLY. Okay. Information security weaknesses have consistently been found at the VA for several years. FISMA compliance helps ensure Congress and the public that the VA is committed to safeguarding veterans' information and VA data. What are the some of the challenges to addressing weaknesses and improving VA's information security programs and practices to comply with FISMA?

Ms. COUNCIL. One of the things, as was mentioned by Mr. Arronte, is the length of some of these repeatable issues. The fact is, we had to put a core process in place. We had to talk about the accountability. We wanted to make sure we were fully sourced, resourced, and that we were also fully funded.

In addition to not only having a team that is out there remediating, we have put a process in place to ensure that these issues stay fixed. I think that is really important. You can't just have it fixed one time and then when auditors come in, they see the same issues.

So what we have done, one of the other new areas that we have added is quality and compliance. Our quality and compliance includes our risk management. The risk management team will get out in front of all of these issues and actually evaluate have we addressed what we said we would address, do the remediation, be engaged with the IG, and make sure that we are hearing what we need to hear in opening, and that our teams are responding properly.

At the end of an audit, we are now also coming back in after we get the audit findings and coming right back into that same organization.

Leaders are being held accountable for any repeatable processes. And in addition, I meet weekly on all security issues with the security top-level pillars to ensure that we continue to make progress.

Since my arrival, we have had five reports open. We had 21 total recommendations. We have closed 95 percent of those already for the OIG. For GAO, we had six reports with 12 total recommendations. Fifty-eight percent of those recommendations are closed or requesting closure. Twenty-five percent of them are on target for closure.

It is a different level of ownership. It is a different level of accountability. We have stressed that every employee is responsible for security. Since that was the key first thing that I committed to do when we arrived, we have set upon a new way of looking at how we do what we do and how we own it.

So our field operations, our information security team, as well as our quality and compliance team, all engage in ensuring that we do not see these material processes continue.

Ms. KELLY. Thank you. My colleague asked about building the work force and what you needed. Once you get them in, how hard is it to keep people because of the competition?

Ms. COUNCIL. I've only been there for 8 months, but I haven't lost anybody. That's a good thing.

I will tell you that there were a number of people that were leaving the organization and they stayed, and I appreciated that, because they really want to make this change.

This is a mission-driven organization. It is all about the veteran. They know that I am here as an appointee because I want to get this right for the veteran. Fifty-six percent of our employees are vets. They get it. They know the value.

So everyone wants to sort of roll their sleeves up and get it right. We just have to make sure we have all the key skills that we need to hold all of our contractors accountable as to what they are delivering.

Ms. KELLY. Okay, thank you so much. My time is up.

Mr. HURD. I will recognize myself for a couple minutes.

Ms. Council, questions to you. In 2009, again, I know this preceded you, the VA abandoned the scheduling improvements it had been working on since 2000 and started over. August 2015, the VA announced it contracted with two companies for a medical appointment scheduling system, the MASS system. And it appears this is like the third try in 15 years at addressing scheduling issues in the VA. Again, I recognize that of that 15 years, you have only been there for 8 months.

What is the current status of the MASS project?

Ms. COUNCIL. There were two parallel processes going on for scheduling. MASS was one, and then there was also a mobile product being developed called VAR, and also updates to VistA called VSE.

VSE and VAR will start rolling out next month in April nationally. They have been piloted. They basically allow the ability to change our scheduling processes.

The current scheduling system is something from—you mentioned COBOL. This is probably from the 1960s. If you could look at it, you will see that it shows the green screen and then also

you'll see that it's an old dot-matrix screen that also doesn't allow people to really know what they are leading to. The VAR and the VSE addresses this.

So far, 95 percent of the users like the new product. And the idea was that if these could not deliver, that we would have through MASS, which was an IDIQ contract, an ability to move forward.

MASS has been put on hold until the Deputy Secretary looks at these new products. Right now, if these new products roll out fine, we will stay with those new products.

The $624 million aligned with MASS. It was never to spend up to that level. Since it is an IDIQ, it is a task order kind of contract. So it was there to support, if these did not work. But we will be rolling out in April with both of those products, one mobile and one into the system.

Mr. HURD. So if VSE and VAR work, we are not going to MASS?

Ms. COUNCIL. They are working today, and if they fully meet our needs—and I think there is also the misnomer on MASS. MASS also includes a workflow and a scheduling capability of room, so it was a much broader look. We wanted something for scheduling right away. And right now, VSE and VAR seem to meet the needs.

Mr. HURD. So are Epic and systems made simple? Are they involved in the VAR and VSE? Or were they to be involved in MASS?

Ms. COUNCIL. They actually are part of the MASS contract.

Mr. HURD. So the folks that are implementing VSE and VAR, are any of them involved in the previous attempts by the VA to do scheduling?

Ms. COUNCIL. Based on the information that we have, no, that would not be the case.

Mr. HURD. I find that a very good thing.

If VSE and VAR are ultimately working, we are going to keep that and it is not potentially going to be grounded by any commercial off-the-shelf systems, correct?

Ms. COUNCIL. Not at this time. That is part of the reason why we are looking for a digital health platform.

The fact is, as you mentioned in your opening remarks, our need to really understand where we need to go for the next 25 years means we really need to make a hard decision and start to think about what we have to do for Care in the Community, what we have to do for ACA, what we have to do for the number of women veterans and make it much more fluid.

Dr. Shulkin, who heads up the VHA, and myself are really just not affecting what we're doing with VistA because VistA 4 is scheduled and it is working, and it is going to roll out as planned into 2018. But to really say, what's the next level of platform? Who should we partner with? How do we make this happen?

We are looking at the work with the DOD to see what they've learned and taking that information and also leveraging it. And we're meeting with industry experts to ensure that what we have in place, what we leave behind when we move on, the next set of leaders can take and move forward with.

Mr. HURD. My last question before we get to Mr. Connolly, how many clinics are currently in this test program using VSE and VAR, rough estimate?

Ms. COUNCIL. This is my account manager at VHA, a new function.

This is rolling out to 10 core as the pilot, and then based on those pilot feedback, it will be going out to the Nation.

Mr. HURD. I would love to know the 10 places it is going, because I would be interested in hearing how it is going from them.

With that, I would like to recognize the distinguished gentleman from the great State of Virginia, Mr. Connolly, for his 5 minutes of questions.

Mr. CONNOLLY. I thank the chairman from the great State of Texas.

Welcome to the panel.

Ms. Council, the VA earned a C rating in the initial scorecard for compliance for FITARA, which actually was one of the higher grades. I would be interested in hearing from you why you think you got, relatively speaking, such a good grade as the baseline. But within that grade were other categories. In data center consolidation, for example, you got an F.

So I wonder if you would, A, just talk a little bit about what your view being relatively new on compliance with FITARA and how FITARA is hopefully a benefit from your point of view, and then secondly, what are you doing about that F in data center consolidation?

Ms. COUNCIL. The FITARA process, at this point, we have put in key processes with the EPMO that I mentioned to you as well as we are doing quality compliance, how we are going about many of the new abilities in data management, which will move us by the end of the year to close to 100 percent on the FITARA. We are excited about it.

I use it as a guidepost. It allows us to really take ownership and hold ourselves accountable for the capabilities that have been put in our hands by having this legislation.

The data center consolidation that you mentioned, we actually reviewed our plan yesterday that, by 2019, we will have eliminated 70 data centers. The other data centers will be eliminated through the use of the cloud, through consolidation of various data processes, and elimination of certain legacy systems. So that is in process.

We are excited because if we can hit everything that we plan on in 2016, we will be the premier governmental agency in FITARA.

Mr. CONNOLLY. Wonderful.

Your aide held up a chart a little while ago on scheduling appointments. Did I understand your answer to the chairman's question was that we are actually still using systems that go back to the 1960s to make scheduling appointments in the VA?

Ms. COUNCIL. I think it is more the late 1970s.

Mr. CONNOLLY. Late 1970s. The Mary Tyler Moore era.

Ms. COUNCIL. Yes.

Mr. CONNOLLY. All right. As opposed to the earlier Dick Van Dyke era.

Ms. COUNCIL. Exactly.

Mr. CONNOLLY. Got it. How vulnerable are those systems to cyberattacks?

Ms. COUNCIL. Last year, I think we blocked something like a 160 million malware attacks in our department.

Mr. CONNOLLY. Wow, 160 million.

Ms. COUNCIL. Yes, sir. We continue to have a defense in-depth capability that we now have reinforced. We are partnered with DHS in a number of key areas and have been very aggressive with moving into some new capabilities.

One of the things that we are always concerned about are any kind of breaches or any concerns with that. What we find is that even in those cases, most of our situations are mailings, information that goes out that shouldn't have gone out to someone in the wrong way.

We also report all of those into the IG. We are aggressive about that, and we will continue to be vigilant. You must be in this kind of space.

Mr. CONNOLLY. I was looking at my own opening statement for today's hearing. In just the last 3 years, the cost to operate and maintain your top four mission-critical legacy IT systems jumped by more than 100 percent for one system and 50 percent for the other three. Is that correct?

Ms. COUNCIL. We will come back to you on that number. I don't know it exactly.

Mr. CONNOLLY. Anyone on the panel that can corroborate those? I'm obviously not Donald Trump. I didn't make that up.

[Laughter.]

Mr. CONNOLLY. Oops. Sorry, Mr. Chairman.

Okay, well, please corroborate. But the reason I cite it is it is indicative of the plight you all have. It is not just trying to maintain legacy systems. It is spending about 80 percent of what we have doing that. It is that the costs get higher every year.

And some of these systems cannot be encrypted and are extremely vulnerable. Now, some of them apparently are in the beyond-encryption period, and the Chinese don't know how to hack into them.

I am told COBOL is one of those categories, Mr. Chairman. So it may have a redeeming unintended consequence.

But the costs are very high. I assume that in your IT budget, most of it is probably spent not on new investments to upgrade services and move to the cloud while at the same time protecting yourself from cyberattacks, 160 million a year, but it is to maintain these legacy systems.

Ms. COUNCIL. To your point, that is one of the reasons that we are looking to move much of the older legacy processes outside of the data center into a cloud process, as well as eliminate them. So the way you eliminate them is by having a real software development lifecycle and really going aggressively after getting those legacies out.

We have in our budget about $18 million this year on getting some of these out. We are also putting in a CMDB. A CMDB is a configuration management database. When you can't see it, and you don't know who owns it, and you don't know how much of it you have, the conversations are very hard to have.

This is going to allow the team to be able to have the conversations and say all of this redline can get out, we don't need it any-

more, or we have another strategy on how we can aggressively address it.

It is a great opportunity for the team. We are going after that, and we hope we will have the CMDB in place by the end of this year.

Mr. CONNOLLY. Mr. Chairman, my time is up, but something you and I talked about, which is we want to find, on a bipartisan basis, ways to incentivize agencies to be able to reinvest in themselves when they identify these savings, and I look forward to as a follow-up to this hearing and others to try to be able to do that. And, of course, Ranking Member Kelly as well. Thank you.

Mr. HURD. Thank you.

The chair notes the presence today of Congressman Seth Moulton of Massachusetts. We appreciate your interest in this topic and welcome your participation.

I ask unanimous consent that Congressman Moulton be permitted to fully participate in today's hearing.

Without objection, so ordered.

And now I recognize the gentleman from Massachusetts for 5 minutes.

Mr. MOULTON. Thank you, Chairman Hurd, for inviting me to this important hearing. This is important because I think our veterans have earned the best health care in the world, and that should be the standard that we are trying to meet.

I get my health care from the VA as a Member of Congress, and I can tell you that I have seen the good and the bad. I have gotten some fantastic doctors.

I had to have surgery back in January and the anesthesiologist and the surgeon who took care of me were incredibly talented. They didn't have to be at the VA. They were there because they wanted to take care of veterans. I felt very comfortable in their care. And then the pharmacy sent me home without the right medications.

There is a veteran in my office named Dennis who gets his care at the VA as well. And he was trying to make an appointment a few weeks ago and couldn't get through on the phone system. Someone else in my office said, you know, you should take a video of this, and the video went viral on Facebook.

Here are some of the comments that we have received on my Facebook page about this video from veterans across the country.

This one from Walcott, Arkansas: "I can tell you this is for real. It happens every time I call. I usually give up and drive to the clinic 18 or 20 miles away so I can talk to a person face-to-face."

From El Paso, Texas: "This is exactly what happens every time you try to call for an appointment or even general information about an existing appointment. This is exactly why lots of us vets end up giving up on the system."

From Colorado Springs: "Finally, a video that shows the frustrations of this process."

And from Philadelphia, Pennsylvania: "The longest I have been on hold with the VA was an hour and 45 minutes before I gave up."

Finally, from Faribault, Minnesota: "I can't count the times this has happened to me. It's enough to make you want to throw the phone through the wall."

So while many have said that they get excellent care once they get into the system, as has been my experience as well, sometimes simply getting access to the system is a real problem.

I know the VA is making progress. I met with the Secretary earlier this week, and I am inspired by his leadership, by the private sector innovation that he is bringing to the organization. But I don't think we have gone far enough.

And it doesn't make sense to me that when people in the private health care system can have access to better scheduling applications, they are not available to veterans. If our standard is that veterans deserve the best health care in the world, because that is what they've earned, then they should have access to these systems as well.

So that is why, Mr. Chairman, I have introduced the Faster Care for Veterans Act with my colleague and friend, Representative Cathy McMorris Rodgers of Washington.

This bill would create a pilot program for the VA to try some of these private sector scheduling programs, currently available technology, and give access to that technology to veterans.

That is the kind of care that I think all of us who use the VA system deserve. And while it seems that the VA is focused on developing their own solutions at great costs and taking enormous amounts of time, it is frustrating to us that we see our friends and colleagues in the private sector using these applications and systems available today.

So with that, I would like to ask Chairman Hurd if I can submit a few questions for the record, and I thank you for inviting me here today.

Mr. HURD. I would like to now recognize Mr. Farenthold from Texas, again for 5 more minutes.

Mr. FARENTHOLD. Thank you very much.

Mr. Moulton hits on an issue.

Mr. HURD. I'm sorry, Mr. Farenthold. Will you yield for one second? I would like to submit for the record two statements, one from the Iraq and Afghanistan Veterans of America, the other one from the American Legion, to illustrate some of the points that Mr. Moulton made.

Without objection, I ask unanimous consent to introduce them into the record.

Without objection, so ordered.

Mr. HURD. Thank you, sir.

Mr. FARENTHOLD. Thank you, Mr. chairman.

Ms. Council, as CIO, the difference between a computer and telephone is basically vanishing today. Does the telephone system fall under your jurisdiction or your leadership as well?

Ms. COUNCIL. Currently, we provide the network capability, but we do not manage the phone contact centers or the contracts of those contact centers.

The issues that are mentioned there, however, we are aggressively working with the new leadership. We have a new leader who put the 311 process in Philadelphia together, who is now coming in. We are making sure that we have the best capability.

I also know that in that particular circumstance that was raised, that vendor who had voicemail now has had the contract updated and there is no voicemail in that process any longer.

So we support it. We are working with them directly. I actually meet with that contact center so that we can ensure that we have the best infrastructure to move us forward more aggressively.

Mr. FARENTHOLD. I understand. This is a call center issue. This is not rocket science. This is technology every company of any size has complete with the ability for overflow calls to potentially go to people's homes or cell phones. We talked about the case of scheduling appointments. There are also tragedies associated with calls being dropped or being sent to a voicemail system that some people didn't even know existed on a suicide prevention hotline.

I would encourage you to work closely with those vendors because, again, I think the line between the IT system and the telephone system really isn't a line anymore, and we ought to be able to use the technology to make sure that no veteran calling for help with suicide has to wait on hold or have their call lost in voicemail.

I'm going to shift gears a little bit. I spend a lot of time in casework. About 70 percent of the casework I do in the district offices that I have in Texas is VA related. Of all the entire government, 70 percent of our complaints and problems are with the VA.

Some folks in the VA need to be kind of hanging their head in shame on that one, I think.

We are spending a lot of time in our office trying to get doctors to work with the VA, see veteran patients under the voucher system or Veterans Choice, and we talked in the first round of questions questioning that you all are working at modernizing that payment system.

But what can we do now? I mean, is there anything that can be done now to get the doctors paid quicker so they will see our veterans again?

The local VA can say, here is help in filling out the forms. Here is how you fill them out right. If it takes too long, call us and we will try to push it through.

But you shouldn't have to call a senior person in the VA or call my office to have my red tape cutter call the VA.

First off, when will it be fixed? And until then, is there anything we can do to improve the situation?

Ms. COUNCIL. I actually will be happy to get some information to you. One of the things about IT, if we really want to be good, we have to know what our business partners are doing. So I know that Dr. Shulkin and Dr. Bally are working very strongly to figure out ways that we can pre-pay for certain things, that we can expedite this process. It is all part of out access process that we need.

We are also looking at proof of concepts around doing some things in the cloud with urgent care and telehealth with urgent care so we can see people the same day, in many cases.

So I will be happy to get some information back to you exactly what they're doing. But I know we are aggressively making some decisions and prepaying in some cases, so that this is not the problem.

Mr. FARENTHOLD. We worked really hard in Congress to get the Veterans Choice program implemented and provide quick care for

veterans. But if you guys can't deliver on paying the doctors, then they don't want to see them. Obviously, a lot of that is contracted out. You have different contractors, but we have to find a way to get this done because there is no point fixing these laws, if you guys can't execute them and do that. So I definitely encourage you to do that.

Finally, we talked a little bit about some of the older systems, your email system, some Windows XP. Do you have a dollar figure on how much it is costing to contract for beyond-lifecycle support on that?

Ms. COUNCIL. I do not, but I can get you that information.

Mr. FARENTHOLD. All right. It would be interesting to look at comparing how much we are paying for that extended support versus how much it would cost to have somebody come in and upgrade an off-the-shelf product that pretty much any decent system integrator in the country ought to be able to put in.

So I see my time is up. I appreciate your commitment. I wish I saw the successes that I hear in your voice reflected at the local level. I am waiting expectantly for that to trickle down, so our veterans don't have to wait for the care that they need. Thank you.

Mr. HURD. Mr. Arronte, do you have any insight on that last question Mr. Farenthold asked about the percentage of how much it costs?

Mr. ARRONTE. No, sir. We don't.

Mr. HURD. Okay, thank you.

I would like to recognize Ms. Kelly for an additional 5 minutes.

Ms. KELLY. How do the projects and programs developed by 18F USDS integrate with other VA systems?

Ms. COUNCIL. The GSA 18F group is I think what you're referring to. We have a digital team that works with us. We actually have one that is doing vets.gov as well as our case appeals modernization.

We are actually meeting with Assistant Secretary Duncan at the EPA and their digital service person to find out how they are using 18F to see if we also have some opportunities where we can leverage them as well.

Ms. KELLY. What steps are taken to ensure that conflict of interest protocols are in place before work by 18F and USDS employees begin at the VA?

Ms. COUNCIL. At this point, I will come back to you on that. Most of those people are hired as Schedule A on the digital services team. We do not have any 18F people at this point, but we do have digital service folks who come in on schedule A, which is about a 2-year, maybe 3, but mostly 2-year expectation. I will come back to you and let you know if there are any conflict of interest forms.

Ms. KELLY. And how are the activities of 18F and USDS audited by the VA?

Ms. COUNCIL. The digital service teams are part of the IT team. We manage their work just like any other employee. Their processes, their systems, they have to adhere to every single process that any other employee has to adhere to. They are not set separate.

Ms. KELLY. Do you have any comments about that?

Mr. ARRONTE. No, ma'am.

Ms. KELLY. Okay.

I yield back the balance of my time. Thank you.

Mr. HURD. Thank you. I am going to recognize myself for 5 minutes.

Mr. Arronte, what are your thoughts on the decision to pursue VAR and VSE and put MASS on hold?

Mr. ARRONTE. I'm going to turn it over to the subject matter expert to discuss.

Mr. HURD. Mr. Bowman?

Mr. BOWMAN. Obviously, VA has had some history of trouble with their scheduling systems, so changes need to be made.

I think the question is whether or not they're worthwhile investments and whether or not they're going to have an immediate impact to help with the scheduling. So pursuing these makes a lot of sense, but whether or not you're going to see an immediate impact, that is really the question.

Mr. HURD. Ms. Council, what immediate impact do you think you are going to see with the deployment of VSE and VAR?

Ms. COUNCIL. The usability of the systems is just so much better than what is currently available. We will make sure we send you the depiction. When you see what is currently available, you will get it right away. I think once I saw that, I understood the difficulty in having to move from screen to screen to check on things to schedule an appointment.

Mr. HURD. So I am still trying to wrap my head around all this. Why pursue this versus trying to get something off-the-shelf that you could possibly deploy a little sooner, especially if we had $624 million available for that? Am I not understanding this correctly?

Ms. COUNCIL. I won't speak on behalf of the Deputy Secretary, but the way it was explained to me was they wanted to make sure that we were going to do something with scheduling, and we didn't want to necessarily believe that if we created it here, we couldn't leverage a piece of software—which by the way, MASS is Epic software.

So the real question is, we were going to do one or the other, and I think what we found is that if we just needed pure scheduling and we needed a mobile capability, we were able to create that and integrate it into VistA very simply. But the team had to try it, make it work, and I think they had an heir and a spare and really wanted to make sure we did the right thing on behalf of the veteran in getting this access dealt with.

But I do not want to put words in the mouth of the Deputy Secretary, but that is how it was explained.

Mr. HURD. So this was the decision by the Deputy Secretary to pursue VSE and VAR over MASS or some other commercial, off-the-shelf technology?

Ms. COUNCIL. It was actually with, and then to run a pilot, and then based on the experiential relationship between that software and this one, which one was really best. But when Dr. Shulkin came in, when I came in, we really wanted to move fast. We wanted to get this access going, and we wanted to go with the fastest solution possible.

As I mentioned, one of the key things that we have to really take a hard look at is the overall digital health platform, not just DHR,

not just continuing to put more money into VistA, but really say we have VistA 4, it is delivering on the things it needs to, it is keeping us in the regulatory responsibility that we have, but what is the new new? What is the thing that we must do to enable the veteran anywhere at any time?

That is probably a platform that is newer, a platform that is based on a COTS type of opportunity. But at this point, by June, Dr. Shulkin and his team would have assessed what we have laid out as a technical opportunity and come back when we have a solution.

Mr. HURD. So is Dr. Shulkin the one responsible for the policies and procedures and workflow and how they handle a call and handle an appointment?

Ms. COUNCIL. Yes, sir.

Mr. HURD. Because ultimately, you are not responsible for scheduling. You are responsible for providing a platform in which other elements of the VA handle this, correct?

Ms. COUNCIL. Yes, sir.

Mr. HURD. Because, again, I think part of the problem is the processes that are in place and you are delivering a system. And if it's not being used properly, we are going to have problems.

Mr. Arronte, do you have any opinions on the implementation of this software and how the other elements of the VA would be able to put the processes in place to ensure they are using this new tool properly?

Mr. ARRONTE. Sir, I think our concern right now is this is new, and so as some of this is still being piloted, we have not conducted any reviews. We plan to, and I'm going to have Mr. Bowman speak about some past experiences.

But what is kind of long standing that we have seen with VA, with IT, they are trying to centralize at the headquarters level. I think the field is not always acceptable of that centralization. So sometimes what we see in some of our previous work is, there is a good plan and it looks good on paper, but getting out of the gate and getting it implemented seems to be some of the issues historically.

Mr. BOWMAN. Anytime VA is involved with software development, it seems to be a high-risk venture. Some of the projects that we have looked at, VA tends to go over budget on cost. They seem to not deliver the intended functionality.

So I think oversight of this project is essential, especially as it impacts veteran scheduling. VA just does not have a good history of delivering systems on time and within budget.

Mr. HURD. How long, Mr. Bowman, have you been part of the IG apparatus looking at the VA?

Mr. BOWMAN. I have been with the IG for over 8 years.

Mr. HURD. So looking back at some of those failures, what would you say were some of the key reasons that those projects failed, with hindsight as a benefit?

Mr. BOWMAN. A theme that comes through is ever-changing requirements. You have the business owners that can't quite decide on what the functionality should be. So there are a lot of changing system requirements, functionality requirements, and that impacts

the development time. It encourages rework, systems under development.

But until you stabilize those requirements, you are really unable to meet any milestones or stay within project cost constraints.

Mr. HURD. Mr. Arronte, do you have any opinion?

Ms. Council, do you have an opinion on what was just stated?

Ms. COUNCIL. Yes, sir. I think Mr. Bowman is correct when you talk about waterfall. As we moved to agile processing and using ITIL as our processes, you will see a marked difference in how we manage and work with our projects.

So for instance, we have implemented what has been called a best practice within the VA around projects and visibility and transparency. All projects on the breakthrough 12, which you might've heard Secretary McDonald speak about, we actually have a governance committee that tracks against those, against resources, schedule, budget, as well as ATO or security.

We see them every week. I see them every week. And we also, if an issue was open, be it a business issue or a resource that we have and it goes longer than 10 days, we call a tech stat, which means they come and I'm there, as well as the head of the application area, as well as our CFO, and we make a decision.

We are no longer waiting until we get the right requirements and keeping these things going. If it is the kind of work that needs to get done, we have asked the businesses to be prepared to do it.

With agile, it is a side-by-side, working real-time relationship in the development of the solution.

We are looking for a new transformation, and I would not attest to anything that the gentleman mentioned in the past. What I will be excited about is what they see in the future.

Mr. HURD. Amen to that.

Mr. Arronte, some of the FISMA violations dating back to 2006: unsecured wireless networks in VA, lack of encryption on sensitive data. Are those two issues that you found that are still problematic?

Mr. ARRONTE. Yes, sir. We have repeat findings and recommendations. Password protection or credentialing, for the last 3 years, they have clearly been repeat findings.

VA's enterprise infrastructure is huge, but some of these recommendations, and I think Ms. Council has addressed that, some of them I think are fairly simple to fix.

Mr. HURD. Yes. For example, Ms. Council, unsecured wireless networks in VA sites, how do you go about fixing that and getting compliant with that in the next few months? Talk me through the process on why something like that takes a while to do.

Ms. COUNCIL. I think at times it probably took longer than it should have. We now have the same assessing software that the IG has, so that we are looking at things in the same way. We make sure that we remediate early and often. We are tracking to those metrics, and we are actually going to grab all those metrics and make sure that we can also depict them out into the organization.

One thing that was just mentioned was the field. In this transformation, we are also reorganizing for the first time what we do in the field. We are putting in a new help desk. We are reassessing and putting in service-level agreements with all of our customers.

We also will have customer relationship managers out in the field that will actually go across all the businesses to understand, is IT doing what it needs to do, and do we have situations where our business partners might need some opportunity in helping them understand how to have a more secure environment?

We are, in addition, laying out a very different way on how we look at how we do services and what people are held accountable for.

In addition, every goal that relates to our strategy is being cascaded into the leader's goals and expectations for the year.

So for us, we recognize exactly what we are hearing is not acceptable. We know now that 95 percent of the things that we used to be in what we call our tick are now covered. Those 5 percent are more linkages between the VA and maybe university and third partners, but even that we need to provide some solutions to. And Brian and his team are doing that.

Mr. HURD. So I think this is my final question.

Moving the Email as a Service, why hasn't that been done before?

I ask that question really to leverage your experience and vision as a tool to work with some of your peers in other departments. It seems so simple. It seems so basic. Why hasn't it been done before?

Ms. COUNCIL. I appreciate the question, because my new Principal Deputy, Ron Thompson, who came from HHS is actually spearheading that new contract. Email as a Service will be our first move, and that should happen in the next 60 days or so, the finalization of that.

We are working with GSA and really trying to get in the FedRAMP kind of environment. We feel that if VBA can participate, we can actually make it good for everyone because of our size, but also leveraging the solutions that are already out there.

So we are looking at those vehicles and moving into them, and the first one is Email as a Service.

Mr. HURD. Great. You mentioned earlier enterprise cybersecurity strategy. We would like love to have a copy of that, if possible.

Ms. COUNCIL. No problem.

Mr. HURD. The committee would love to have that.

As Congressman Farenthold mentioned, all of us in Congress are dealing with veterans' issues and the lack of service and their frustrations. I think you recognize the importance of your role, because you and your team and OI&T can really be the units that transform how the VA delivers a service.

I appreciate your vision. I hope we have you around long enough in order to see that vision come through.

And know, on the employees and making sure you can hire and retain good employees, we are trying to work on ways to make that more flexible. We are trying to work on ways on how IT procurement can be streamlined so you can move quicker.

My friend Colonel McSally, Congresswoman McSally, always says the bad guys are moving at the speed of light, and we are moving at the speed of bureaucracy. If we can fix that, it will go a long way in order to serve those folks that have been willing to put themselves in harm's way in order to keep us safe at night.

So I want to thank you all for being here today. I would also like to thank the ranking member for always indulging my going over time and for her willingness to work together on such an important issue.

And thank you for taking the time to appear before us today.

If there is no further business, without objection, the subcommittee stands adjourned.

[Whereupon, at 3:14 p.m., the subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Wednesday, March 16, 2016
2 p.m. – Rayburn 2247
Congressman Gerald E. Connolly (VA-11)

Oversight Subcommittee on Information Technology:
"VA Cybersecurity and IT Oversight"

Mr. Chairman, I appreciate today's opportunity to hear from the Department of Veterans Affairs on its information technology management and modernization, specifically its efforts to strengthen cybersecurity and to implement the Federal Information Technology Acquisition Reform Act, which is better known as FITARA or Issa-Connolly. The VA provides health care, financial support, and other benefits to the millions of men and women who served our nation in uniform and their families, and few federal agencies could benefit more from widespread deployment of secure, reliable IT solutions. In fact, today's discussion follows a joint hearing we held with the Veterans Affairs Subcommittee on Oversight and Investigations last fall on the efforts within the VA and the Defense Department to achieve interoperability in their electronic health records.

While the VA's Chief Information Officer, Ms. Laverne Council, should be commended for her efforts to advance IT reforms within the department since her appointment last July, she is faced with multiple challenges. For starters, there is the sheer scope of the VA's IT portfolio with hundreds of hospitals, clinics, and offices scattered in communities across the country staffed by more than 7,500 IT professionals and supported by more than 5,500 contractors. Continuously monitoring cyber threats and authorized network access is paramount with so many potential vulnerabilities. The department is also wrestling with the costs of maintaining its aging legacy systems on which most of its core functions, such as financial management and tracking of benefits, are built. In just the last three years, the cost to operate and maintain its top four mission-critical legacy IT systems jumped by more than 100 percent for one system and nearly 50 percent for the rest. As my colleagues are well aware, there also is a deficit of public confidence in the VA. Modernizing IT systems to improve service delivery will no doubt help restore some of that trust, but the current public perception remains a hurdle that must be overcome.

In its 2015 High Risk Report, the Government Accountability Office added two new areas of concern. The first was, "Managing Risks and Improving Veterans Affairs (VA) Health Care," which specifically noted IT failures that have limited the department's effectiveness in serving our veterans. In addition to referencing the ongoing health IT interoperability effort that was the subject of our prior hearing, the GAO also noted the VA's failed effort to replace its outpatient appointments scheduling system, which was finally terminated after it spent 9 years and $127

million. The GAO specifically cited "weakness in project management and a lack of effective oversight."

That leads to the second new addition to the High Risk List, "Improving Management of IT Acquisitions and Operations," in which GAO recognizes the potential of our bipartisan FITARA legislation to achieve cost-savings and cost-avoidances by strengthening agency CIO authorities, facilitate the use of best practices in IT management, and promote the elimination of wasteful and duplicative IT systems. In fact, Comptroller General Gene Dodaro said in Congressional testimony, "...one of the reasons that we put IT acquisitions and operations on the list is in order to elevate attention to make sure that FITARA, the Issa-Connolly bill, is implemented effectively."

Our legislation represents the first major reform of the laws governing federal IT management since the seminal Clinger-Cohen Act of 1996. I appreciate this Subcommittee's efforts to hold regular hearings to gauge agency progress. Last fall we created an initial scorecard measuring each agency's progress in implementing the various components of FITARA. That first assessment focused on four of seven major reform activities: Data Center Consolidation, IT Portfolio Review Savings, Incremental Project Development/Delivery, Risk and Assessment Transparency. These metrics were chosen because their implementation will have a demonstrable benefit for improving IT acquisitions and operations.

The VA earned a "C" rating, one of the higher marks for all agencies. One area in which the VA has improved is charting incremental development and holding project managers more accountable. Under the new CIO enhancements, FITARA requires projects to be developed incrementally and to provide more frequent reporting to identify any that are behind schedule or perhaps no longer meeting department objectives. Without question that tool would have been useful in managing the failed outpatient scheduling system. The VA now reports that 99 percent of its active projects are being delivered incrementally. The new Enterprise Program Management Office created within the VA Office of Information and Technology is implementing this and other reforms. Rather than ad hoc management, the VA is now using portfolio-based management, and it has dramatically reduced its document production requirements, streamlined its decision making process, and shortened its delivery timelines. That is laudable progress, and I encourage Ms. Council and her team to continue pursuing the other efficiencies under FITATA, particularly data center consolidation.

OGR Committee Subcommittee on Information Technology
Hearing on VA IT and Cybersecurity Oversight
Rep. Cathy McMorris Rodgers | March 16, 2016

Thank you Chairman Hurd, and Ranking Member Kelly, for allowing me to participate in today's hearing on this important topic.

Without a doubt, we were all shocked and horrified when the news broke several years ago that some VA employees were manipulating wait times and keeping secret waiting lists for veterans seeking appointments with the VA.

The result was that veterans who desperately needed care faced unacceptably long wait times, poor treatment, and failed customer service at VA facilities across the country. **Several even died while waiting for appointments.**

But instead of steadily shorter wait times, the number of veterans waiting 30 days or more for medical care has increased – up 50 percent last year. That's simply not acceptable.

The solution will require a fundamental shift in the culture and day-to-day management at the VA.

I've heard from a number of veterans in Washington State, and here's what I can tell you: They want to be empowered – empowered to make their own health care decisions, while giving VA employees more tools to do their jobs effectively and efficiently.

To help with this, Congressman Moulton and I have introduced H.R. 4352, the Faster Care for Veterans Act, which would require the VA to conduct a pilot program using existing, commercially-available online patient self-scheduling capability that allows patients to schedule, confirm, and modify appointments in real-time.

That means veterans could schedule appointments 24 hours a day, 7 days a week, and even backfill open appointments that had been previously scheduled but then cancelled.

For 15 years now, the VA has attempted to improve its scheduling processes. Despite millions of taxpayer dollars invested in these experiments, they essentially started over in 2010.

Now, the VA plans to spend an additional $624 million over the next five years to develop a new scheduling system, the utility of which is unclear at best.

If the VA is unable to fulfill President Lincoln's promise to "care for him who shall have borne the battle," then we must encourage the VA to try something different, and equip them to succeed.

Self-scheduling is only one example of the endless creative and innovative ideas at our disposal.

The Faster Care for Veterans Act is about empowering veterans who have sacrificed so much in defense of our nation, sooner rather than later, in a cost effective manner.

This bill is pro-veteran and pro-transparency. With this bill, we are demonstrating to the VA that innovative technology -- already being used in doctors' offices across the country -- can also work for them to:

> Cut back on the red tape; Stay within budget; and get our veterans the care they've earned and need.

I want to thank Congressman Moulton for partnering with me on this effort, and Chairman Hurd for cosponsoring our bill.

I look forward to hearing how and when the VA plans to bring its scheduling system into the 21st Century so that veterans get the care they need, when they need it.

Thank you again, Mr. Chairman, for holding this hearing and allowing me to join you today. I yield back the balance of my time.

Statement for the Record
by
Elizabeth Welke, J.D.
Associate of Political and Intergovernmental Affairs
of
Iraq and Afghanistan Veterans of America
before the
House Oversight and Government Reform Committee
Subcommittee on Information Technology
hearing on
VA Cybersecurity and IT Oversight

March 16, 2016

Chairman Hurd, Ranking Member Kelly and Distinguished Members of the Subcommittee, on behalf of Iraq and Afghanistan Veterans of America (IAVA) and our more than 450,000 members and supporters, we would like to extend our gratitude for the opportunity to share our views and recommendations regarding oversight of information technology at the Department of Veterans Affairs (VA), but focusing more specifically on the deficiencies with the VA's current scheduling systems.

Just under a year and a half ago, whistleblowers revealed a wait-list at the Phoenix VA hospital that rocked the veterans community and the nation. It was revealed some employees engaged in the manipulation of wait times. The scandal did not stop in Phoenix; 110 VA facilities across the country also kept secret lists in order to hide wait times. Congress responded with the Veterans Access, Choice and Accountability Act (VACAA) in order to empower VA to clean up its personnel problems. However, personnel problems were only the beginning. Deficiencies with the VA's current scheduling systems have also

caused the VA to fall short of meeting the needs of today's veterans as a government agency stuck in the twentieth-century.

Approximately 60 percent of those who have served in Iraq or Afghanistan are enrolled in the VA health care system. Many of these veterans have returned home having survived complex injuries that require a dynamic approach to health care. Unfortunately, they often face long wait times -- from several months to over one year. Many of our members have reached out to us expressing concern and frustration with this particular problem. Too often, veterans feel they are fighting a system for the benefits they have earned.

One Navy veteran and IAVA member leader who served in Iraq waited three months for an initial appointment for mental health treatment for PTSD from the New Orleans VA. She then waited an additional two months when she requested a follow-up appointment. She reached out to IAVA and a representative contacted the Louisiana VA on her behalf, but never received a response. This veteran said she simply cannot count on the current appointment system in a time of need.

Two years ago, an IAVA member and disabled veteran developed a lump on his neck. Several months later, the VA decided to surgically remove the mass and told him that the biopsy showed it was benign. One year later, the VA notified the veteran this was a mis-diagnosis: the tumor was malignant. Most recently, he waited three months for an appointment. He is still in a state of limbo.

A Marine veteran of Iraq and two-time Purple Heart recipient reached out to IAVA reporting a mental health crisis and suicidal ideation. He had previously

called the Veterans Crisis Line, which referred him to his local VA where he had a psychiatrist and a therapist. The veteran was told by his VA he could not be seen by his doctors for nearly three months, even though he was reporting a mental health crisis.

Another IAVA member, a medically-retired Marine Corps infantryman, was experiencing visual and auditory hallucinations as a result of PTSD. When a particularly difficult episode left him unable to work, it took him three weeks to talk to someone, and he was told it would take thirteen months to get a mental health consultation at the Houston VA. Over the course of two tours in Iraq, this Marine had survived 24 roadside bombs, yet he said the VA was still more difficult to navigate.

Unfortunately, these stories are not uncommon. According to IAVA's most recent member survey, 41 percent of our members have reported having challenges with scheduling appointments. Over 10 percent state that they feel "continually frustrated" with the current system; however, when these veterans do receive VA health care, they are largely satisfied with the quality. Clearly, access to timely care would improve VA services overall.

Today's veterans envision a system designed with the same can do spirit required of them during their service. While there is a lot of work to be done to fully reform the VA, the bipartisan *Faster Care for Veterans Act of 2016* (H.R. 4352) introduced by Reps. Seth Moulton and Cathy McMorris Rodgers takes a positive, tangible step toward improving the scheduling deficiencies at the VA. Many of us watched the recent viral video of a member of Rep. Moulton's staff who served in Iraq, trying to schedule an appointment at his local VA hospital in Massachusetts, before walking away in frustration after endless automated

phone messages.

H.R. 4352 takes a strong step to address the scheduling challenge by directing the VA to begin an 18-month pilot program in at least three Veterans Integrated Service Networks (VISNs) under which veterans use a website to schedule and confirm appointments at VA medical facilities.

All veterans deserve the highest standard of quality and timely care, so IAVA has called for use of new technologies to streamline VA scheduling processes and enable the VA to take a more dynamic approach to respond to veteran needs. The online self-scheduling system envisioned in H.R. 4352 will offer the VA a more efficient process that enables them to better meet this standard.

IAVA members, and all veterans, deserve the very best our nation can offer when it comes to fulfilling the promises made to them upon entry into the military. We hope this Subcommittee takes into consideration our concerns and implements the recommendations laid before you today.

Statement for the Record
Iraq and Afghanistan Veterans of America
before the
House Oversight and Government Reform Committee
Subcommittee on Information Technology
Wednesday, March 16, 2016

Biography of Elizabeth Welke, J.D.
Associate of Political and Intergovernmental Affairs
Iraq and Afghanistan Veterans of America

Elizabeth Welke is the Associate of Political and Intergovernmental Affairs at the Iraq and Afghanistan Veterans of America (IAVA) where she supports the development of IAVA's annual policy agenda and advocacy campaigns and helps lead IAVA's engagement with other Veteran Service Organizations, government agencies and advocacy organizations. Elizabeth received her Bachelor of Arts in Political Science from the University of Iowa, Iowa City, IA and holds a J.D. from Regent University School of Law, Virginia Beach, VA. She is the proud wife of a U.S. Marine Corps veteran who served in Operation Iraqi Freedom from 2005-2006.

Statement on Receipt of Grants or Contract Funds

Neither Mrs. Welke, nor the organization she represents, Iraq and Afghanistan Veterans of America, has received federal grant or contract funds relevant to the subject matter of this testimony during the current or past two fiscal years.

Statement for the Record
by
Elizabeth Welke, J.D.
Associate of Political and Intergovernmental Affairs
of
Iraq and Afghanistan Veterans of America
before the
House Oversight and Government Reform Committee
Subcommittee on Information Technology
hearing on
VA Cybersecurity and IT Oversight

March 16, 2016

Chairman Hurd, Ranking Member Kelly and Distinguished Members of the Subcommittee, on behalf of Iraq and Afghanistan Veterans of America (IAVA) and our more than 450,000 members and supporters, we would like to extend our gratitude for the opportunity to share our views and recommendations regarding oversight of information technology at the Department of Veterans Affairs (VA), but focusing more specifically on the deficiencies with the VA's current scheduling systems.

Just under a year and a half ago, whistleblowers revealed a wait-list at the Phoenix VA hospital that rocked the veterans community and the nation. It was revealed some employees engaged in the manipulation of wait times. The scandal did not stop in Phoenix; 110 VA facilities across the country also kept secret lists in order to hide wait times. Congress responded with the Veterans Access, Choice and Accountability Act (VACAA) in order to empower VA to clean up its personnel problems. However, personnel problems were only the beginning. Deficiencies with the VA's current scheduling systems have also

caused the VA to fall short of meeting the needs of today's veterans as a government agency stuck in the twentieth-century.

Approximately 60 percent of those who have served in Iraq or Afghanistan are enrolled in the VA health care system. Many of these veterans have returned home having survived complex injuries that require a dynamic approach to health care. Unfortunately, they often face long wait times -- from several months to over one year. Many of our members have reached out to us expressing concern and frustration with this particular problem. Too often, veterans feel they are fighting a system for the benefits they have earned.

One Navy veteran and IAVA member leader who served in Iraq waited three months for an initial appointment for mental health treatment for PTSD from the New Orleans VA. She then waited an additional two months when she requested a follow-up appointment. She reached out to IAVA and a representative contacted the Louisiana VA on her behalf, but never received a response. This veteran said she simply cannot count on the current appointment system in a time of need.

Two years ago, an IAVA member and disabled veteran developed a lump on his neck. Several months later, the VA decided to surgically remove the mass and told him that the biopsy showed it was benign. One year later, the VA notified the veteran this was a mis-diagnosis: the tumor was malignant. Most recently, he waited three months for an appointment. He is still in a state of limbo.

A Marine veteran of Iraq and two-time Purple Heart recipient reached out to IAVA reporting a mental health crisis and suicidal ideation. He had previously

called the Veterans Crisis Line, which referred him to his local VA where he had a psychiatrist and a therapist. The veteran was told by his VA he could not be seen by his doctors for nearly three months, even though he was reporting a mental health crisis.

Another IAVA member, a medically-retired Marine Corps infantryman, was experiencing visual and auditory hallucinations as a result of PTSD. When a particularly difficult episode left him unable to work, it took him three weeks to talk to someone, and he was told it would take thirteen months to get a mental health consultation at the Houston VA. Over the course of two tours in Iraq, this Marine had survived 24 roadside bombs, yet he said the VA was still more difficult to navigate.

Unfortunately, these stories are not uncommon. According to IAVA's most recent member survey, 41 percent of our members have reported having challenges with scheduling appointments. Over 10 percent state that they feel "continually frustrated" with the current system; however, when these veterans do receive VA health care, they are largely satisfied with the quality. Clearly, access to timely care would improve VA services overall.

Today's veterans envision a system designed with the same can do spirit required of them during their service. While there is a lot of work to be done to fully reform the VA, the bipartisan *Faster Care for Veterans Act of 2016* (H.R. 4352) introduced by Reps. Seth Moulton and Cathy McMorris Rodgers takes a positive, tangible step toward improving the scheduling deficiencies at the VA. Many of us watched the recent viral video of a member of Rep. Moulton's staff who served in Iraq, trying to schedule an appointment at his local VA hospital in Massachusetts, before walking away in frustration after endless automated

phone messages.

H.R. 4352 takes a strong step to address the scheduling challenge by directing the VA to begin an 18-month pilot program in at least three Veterans Integrated Service Networks (VISNs) under which veterans use a website to schedule and confirm appointments at VA medical facilities.

All veterans deserve the highest standard of quality and timely care, so IAVA has called for use of new technologies to streamline VA scheduling processes and enable the VA to take a more dynamic approach to respond to veteran needs. The online self-scheduling system envisioned in H.R. 4352 will offer the VA a more efficient process that enables them to better meet this standard.

IAVA members, and all veterans, deserve the very best our nation can offer when it comes to fulfilling the promises made to them upon entry into the military. We hope this Subcommittee takes into consideration our concerns and implements the recommendations laid before you today.

Statement for the Record
Iraq and Afghanistan Veterans of America
before the
House Oversight and Government Reform Committee
Subcommittee on Information Technology
Wednesday, March 16, 2016

Biography of Elizabeth Welke, J.D.
Associate of Political and Intergovernmental Affairs
Iraq and Afghanistan Veterans of America

Elizabeth Welke is the Associate of Political and Intergovernmental Affairs at the Iraq and Afghanistan Veterans of America (IAVA) where she supports the development of IAVA's annual policy agenda and advocacy campaigns and helps lead IAVA's engagement with other Veteran Service Organizations, government agencies and advocacy organizations. Elizabeth received her Bachelor of Arts in Political Science from the University of Iowa, Iowa City, IA and holds a J.D. from Regent University School of Law, Virginia Beach, VA. She is the proud wife of a U.S. Marine Corps veteran who served in Operation Iraqi Freedom from 2005-2006.

Statement on Receipt of Grants or Contract Funds

Neither Mrs. Welke, nor the organization she represents, Iraq and Afghanistan Veterans of America, has received federal grant or contract funds relevant to the subject matter of this testimony during the current or past two fiscal years.

○