AMENDED PASSBACK

STATEMENT OF
MR. SCOTT BLACKBURN
EXECUTIVE IN CHARGE FOR INFORMATION AND TECHNOLOGY
OFFICE OF INFORMATION AND TECHNOLOGY (OIT)
DEPARTMENT OF VETERANS AFFAIRS (VA)
BEFORE THE
SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION
COMMITTEE ON HOMELAND SECURITY
AND
SUBCOMMITTEE ON INFORMATION TECHNOLOGY
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES

March 20, 2018

Good Afternoon, Chairmen Ratcliffe and Hurd, Ranking Members Richmond and Kelly, and Distinguished Members of the Subcommittees. Thank you for providing me with this opportunity to discuss the status and progress that VA's OIT is making towards its deployment of the Federal Government's Continuous Diagnostics and Mitigation (CDM) Program and our Information Technology (IT) modernization effort. I am pleased to be joined today by Mr. Dominic Cussatt, Chief Information Security Officer, and Mr. Gary Stevens, (Acting) Deputy CISO, Executive Director Policy and Strategy.

The health, safety, welfare, and prosperity of our Veterans are our highest priorities at VA. As one of five siblings who is either a Veteran or still serving in uniform and are all at least the fourth generation of U.S. military Veterans in our family, I take personal pride every day in fulfilling VA's sacred mission, and believe in making VA the best choice for Veterans. We want all Veterans to choose VA like I have, not because it is their only choice, but because we are the best at what we do.

It is an exciting time to be leading OIT with all of the significant strides we are making in information technology. VA is making progress in its cybersecurity and modernization initiatives as well as with Federal Information Technology Acquisition Reform Act (FITARA) and Federal Information Security Management Act (FISMA) compliance. We have announced our intention and will soon be moving forward to replace our decades-old VistA platform with a modern Electronic Health Record (EHR) that will achieve full intra-VA and VA-Department of Defense (DoD) interoperability. The new EHR will also provide the capability for much improved interoperability with community partners. This will be an important development since over 30 percent of our care is currently done outside the Veterans Health Administration (VHA) system in the community.

VA recently announced the launch of a "beta" version of its Lighthouse Lab, a computer platform offering software developers access to tools for creating mobile and

web applications that will help Veterans better manage their care, services, and benefits. Eleven leading health care systems have agreed to sign a VA Open Application Programming Interface (API) pledge to accelerate the mapping of health data to industry standards, including the current and future versions of Fast Healthcare Interoperability Resources (FHIR).

VA is continuing to expand telehealth and self-service options, such as online scheduling, to improve the Veterans experience. We are pushing aggressively on our "buy first" strategy using commercial off-the-self solutions to replace expensive and outdated systems. Next week, we will launch a new cloud-based, Software as a Service (SaaS) IT service management tool, which will standardize the delivery of IT services and provide our employees with an efficient and consistent end-user experience.

This is the second time in the past several months OIT leadership has appeared before the House Oversight and Government Reform IT Subcommittee. On December 7, 2017, we discussed the progress VA was making towards its transformation efforts, notably our IT modernization effort; FITARA and FISMA compliance; the Electronic Health Record Modernization (EHRM) initiative; and Enterprise Cybersecurity Strategy (ECSS). My testimony today will cover some of those topics with a specific emphasis on the status and progress of the CDM rollout and our IT modernization efforts.

ENTERPRISE CYBERSECURITY STRATEGY PROGRAM (ECSP)

VA, our core constituents, and our external partners are subject to a wide range of cyber threats. Given the high degree of connectivity, interdependence, and reliance on integrated open platform technology, meeting cybersecurity challenges requires strategic attention and collaboration across the VA ecosystem.

Within OIT, we are committed to protecting Veteran information and VA data, as well as limiting access to only those with the proper authority. This commitment requires us to think agency-wide about security holistically. To achieve this end, VA Office of Information Security (OIS) manages cybersecurity risk through VA's ECSP to enable VA to securely fulfill our mission and protect VA information systems.

As part of the ECSP, VA's Enterprise Cybersecurity Strategy is being refreshed to reinforce VA's strategic goals and objectives that inform cybersecurity behaviors at VA. Our principles include, but are not limited to, protection of VA data and Veteran information, evolving VA's resiliency to better adapt to advanced cyber threats, identification and strengthening mission critical systems and infrastructure, modernizing IT, overseeing a secure operational environment, and the recruitment, development, and retention of a talented cybersecurity workforce.

With the establishment of ECSP, we are embarking on a change in mindset of how to manage cyber risk. Through ECSP, we will make prioritized, defensible decisions related to the implementation of cybersecurity projects (that may be technical

or procedure-based), align programmatic activities with the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), and create an integrated and transparent program across each level of the program, which includes government-wide statutory requirements, VA policy and implementation guidance, organizational cybersecurity capabilities, mission/business processes, and the information system level.

We have recently focused on the following:

- Plans of Action created in response to the fiscal year (FY) 2015 Office of Inspector General FISMA audit, which have been closed as of December 31, 2017.
- Eight Strategic Domains created as a result of VA's 2015 Enterprise Cybersecurity Strategy following the release of the Office of Management and Budget (OMB) Cybersecurity Implementation Plan on October 30, 2015.

VA's ECSP is another step forward in VA's commitment to safeguarding Veteran information and VA data within a complex environment. Our strategy establishes an ambitious, yet carefully-crafted approach to cybersecurity and privacy protections that helps 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.

VA INFORMATION SECURITY CONTINUOUS MONITORING (ISCM) AND CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM)

ISCM at VA

In the fall of 2017, we approved our VA ISCM Strategy and the associated ISCM Integrated Project Team (IPT) Charter. The ISCM Strategy and IPT Charter guides VA's continuous monitoring program moving forward detecting and safeguarding systems and data, patient safety, and assisting Veterans after their military career.

Our ISCM program supports a comprehensive VA organizational risk management program. Aligning ISCM to VA's IT risk management program and, in turn, the enterprise risk management program, will provide cost-effective risk management across the organization. ISCM IPT will pursue the following actions to realize this objective:

- Align ISCM activities with risk management activities to provide VA with comprehensive awareness of the security posture and IT infrastructure, assets, and data.
- Align ISCM activities with the ongoing authorization process as it is developed, so information systems security controls are evaluated with data to maintain their ongoing authorization status.
- Implement a process to identify and prioritize critical ISCM data to collect and monitor, and allow ISCM data to support security control assessments.

- Validate that the ISCM strategic planning process is adequately documented. The ISCM strategic planning process should be transparent and communicated to ISCM stakeholders.

OIT will integrate the current and upcoming ISCM capabilities to effectively evaluate VA's information system posture across the agency. This is accomplished through developing and deploying an end-to-end architecture. ISCM capabilities are being automated to the extent possible by leveraging the Department of Homeland Security (DHS) CDM program, while recognizing some security controls cannot be monitored by automated means. Integrating CDM capabilities into the overall ISCM capabilities and augmenting as necessary with automated and manual monitoring will give VA the ability to meet Veteran and operational needs. As ISCM evolves, the frequency of monitoring security controls and collecting measurement data stated in VA policy and procedures will be reviewed and revised.

VA's ISCM strategy outlines processes for updating VA directives, handbooks, and standard operating procedures accordingly to align to the ISCM strategy. VA's strategy will be enacted through updates to VA Handbook 6500, *Risk Management Framework for VA Information Systems*, VA Handbook 6500.3, *Assessment, Authorization, and Continuous Monitoring of VA Information Systems*, and associated ISCM procedures. These documents provide ISCM policy and procedures, in accordance with the NIST Special Publications (SP) 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*. VA Handbook 6500.3 was created to establish requirements and responsibilities for VA to confirm compliance with Assessment and Authorization and continuous monitoring requirements for VA information systems as required by FISMA.

Monitoring tools used for ISCM, CDM, and legacy controls are integrated to achieve data synchronization, elimination of data error, and minimization of human interaction. OIT deploys a variety of tools to maintain situational awareness of VA's security posture. Integrating these monitoring tools across VA is the initial action in automating the monitoring, reporting processes. One of the goals of VA's ISCM strategy is to integrate existing and planned ISCM capabilities in order to form a monitoring solution for VA. This includes integrating existing capabilities such as the VA Cyber Security Operations Center Security Incident and Event Manager and the VA Governance, Risk Management, and Compliance tool into CDM dashboards, as part of Phase 1 of CDM development at VA. Integrating these capabilities and others will inform data analysis and reporting on the effectiveness of VA's ISCM program.

The VA ISCM strategy incorporates a variety of performance measures designed for evaluating the effectiveness of our program. Our program measurement sources include:

- **FISMA ISCM Program Maturity Model:** Summarizes the status of the ISCM program and its maturity based on a five-level scale.
- **FY 2017 Chief Information Officer FISMA Metrics:** Used to assess Federal cybersecurity programs on the progress of their program implementation.

- **NIST CSF:** Provides guidance on cybersecurity metrics and measurements.
- **VA Enterprise Security Architecture:** Informs ISCM measures regarding the maturity of current capabilities.

Looking forward, we are seeking additional stakeholders across OIT to join our ISCM IPT to provide insight into how VA currently tracks and reports ISCM-related data. Our IPT stakeholders will assist in the identification of existing ISCM tools, capabilities, and projects to provide a clear indication of how VA currently monitors its network. Ultimately, a more diverse set of stakeholders across our ISCM IPT will enable various groups across VA to work in concert on future ISCM efforts, while also providing varied inputs in order to confirm we are weighing multiple options when our IPT comes to key decision points.

CDM at VA

CDM is a dynamic effort and the needs of different agencies vary. VA's CDM program is a piece of the larger VA ISCM strategy. The VA CDM program covers 15 continuous diagnostic capabilities, which are distributed across its four phases:

- **Phase 1:** Identify assets on VA network.
- **Phase 2:** Identify and monitor users on the network.
- **Phase 3:** Identify what is happening on the network as well as ways to protect it.
- **Phase 4:** Identify risks on an ongoing basis, prioritize risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

VA would like to provide a more in-depth breakdown of where we are within Phase 1 of our CDM program:

- **Hardware Asset Management (HWAM) -** We are currently implementing HWAM tools and integrating these tools to assist in identifying Internet Protocol addresses across the VA network and is intended to assist in the classification of systems and provide reports to our central dashboards. This work covers approximately 2,500 facilities including hospitals, Benefit Centers, Information Technology Centers, VA Central Office, Data Centers, and others.
- **Software Asset Management (SWAM) -** We are currently implementing our SWAM tool, which is designed to inventory software used in the agency and report the information to our central dashboards. Our team is creating lessons learned from HWAM and analyzing them prior to rolling these tools out.
- **Configuration Settings Management (CSM) -** Our team is currently analyzing existing systems. We are identifying security configuration benchmarks that exist for each IT asset type.
- **Vulnerability Management (VUL) -** We are currently implementing our Dashboards, so we can eventually feed into the DHS Federal Dashboard.

We are also documenting and defining existing network hardware, applications, security products, and configuration control settings currently deployed across the agency in order to further understand the activity across the network. OIT is in the

midst of providing visibility into the reporting endpoints and depicting them on a CDM dashboard to assist in vulnerability management
.

The central dashboards will provide actionable information from HWAM, SWAM, and other security tools for timely remediation of known vulnerabilities as well as transmit data to a DHS Federal dashboard.

OIT documents and provides DHS and OMB its decision on the implementation of any whitelisting applications under the DHS CDM Program, as well as identifies a timeline for its implementation. If VA chooses a non-DHS whitelisting solution, VA delineates the solution selected, the associated timeline for its implementation, and the integration mechanism for the CDM Agency Dashboard. The agency also lists milestones for improving VA's performance in detecting and blocking unauthorized devices and software.

Apart from the updates on Phase 1, we would also like to touch upon our progress in implementing Phase 2 of our CDM Program.

VA conducted requirements sessions with VA Stakeholders, based on the guidance provided by DHS, in order to prepare the CDM Phase 2 Business Requirements Document (BRD). The CDM Phase 2 BRD has been developed and is currently under review. VA has identified the following authoritative data sources to support the four core CDM functions within the agency.

We will continue to collaborate across VA, with DHS, and with our partners across the Federal Government in order to progress ISCM and CDM at VA. We will leverage lessons learned and update our strategies and policies in order to remain in lockstep with Federal statutes and guidance. We will look to use the latest advancements in technology, while also prioritizing security, in order to protect VA data and the Veteran.

OIS POLICY MILESTONES

Recently, we have achieved various policy milestones on the path to further advancing the VA cybersecurity program. These updates in policy allow VA to strategically leverage technologies, which will better serve the Veteran, while also confirming security is prioritized in order to protect the Veteran and VA data.

Cloud activity continues to grow across Federal agencies. In order to prioritize security and allow our stakeholders to use the latest technologies, we have established the following:

- **Cloud Security Framework:** The use and adoption of cloud computing provide great benefits to our mission of serving our Veterans. VA's cloud security framework defines comprehensive and synchronized capabilities to identify and

manage cloud security risks, protect access to our cloud environment, protect cloud applications and data, secure cloud network configuration and connectivity, oversee the physical environment security, monitor the cloud environment, and provide the ability to rapidly respond and recover from a cybersecurity event. These cloud security capabilities address security concerns, and allow VA to capture benefits from cloud computing to serve the Veteran while protecting Veteran and VA data.

- **Cloud Security Guidance:** Our Cloud Security Guidance, which aims to provide guidelines and the minimum requirements, is intended to mitigate the risk associated with increased attack surface for cloud-based systems. Cloud Service Providers are especially vulnerable to attackers due to the value and quantity of data being stored in the cloud. Multi-tenancy increases this risk as VA will not have control of or insight into the security posture of other tenants. Due to lack of familiarity with cloud, misconceptions about the shared responsibility model, and a history of breaches in government cloud systems due to their misconfiguration, VA shall employ cloud-centric defense-in-depth to help reduce these risks.

We have instituted VA Handbook 6500.11, *VA Firewall Configuration*, a firewall policy to cover new technologies in coordination with the Office of Cybersecurity Policy and Compliance. This policy reflects firewall configurations, which are required to comply with the provisions of FISMA and other related information security requirements promulgated by NIST and OMB. We have published VA Directive and Handbook 6513: *Secure External Connections*, which governs the process for managing and continuously monitoring VA connections.

IT MODERNIZATION

Foundation of Modernization

Secretary Shulkin is committed to this vision and making VA a world-class organization. Whether it is from silos to collaboration, or from process to Veteran outcomes, or from guarded to transparent, we are changing the culture at VA. For OIT, that means we must innovate and modernize to provide the best services possible. Modernizing our technology plays a huge role in helping us achieve this objective. That means looking differently at how we provide services to Veterans insofar as how we streamline our approach to take advantage of new technology and industry best practices; improve the ways we deliver care, benefits, and services to Veterans; and how we embrace change and refocus on why and how we serve Veterans.

VA OIT Modernization Strategy

The mission of VA OIT is to collaborate with our business partners to create the best experience for all Veterans. OIT's three goals—Stabilize and Streamline Processes; Eliminate Material Weaknesses; and Institutionalize New Capabilities—drive our strategy and outcomes. They are enduring and will continue to frame our plans for

2018 and beyond. VA OIT approaches everything through our core values of transparency, accountability, innovation, and teamwork. Values we seek to embody, every day, in every project, and for every Veteran.

OIT is committed to VA's I-CARE (Integrity, Commitment, Advocacy, Respect, and Excellence) values and the underlying responsibility to provide the best level of care and services to our Veterans. We expect nothing less and will not tolerate employees who deviate from those core values.

Our comprehensive IT Plan is the foundation for reducing our reliance on legacy systems, and creating new capabilities for a modern VA by leveraging cloud, digital platforms, while incorporating other modern and innovative technologies such as expanded telehealth, robotics, Artificial Intelligence, mobile devices, machine learning, Blockchain, and digital services to increase access, engagement, and interoperability. Through this plan, we will stop or migrate 240 of our 299 projects over the next 18 months, and leverage a buy-first strategy—getting us out of the software development business and ensuring we are positioned to manage the influx of new technologies. We will ensure that we have end-user accessibility of these systems to be Section 508 compliant.

VA is investing in innovative solutions and industry best practices to build a stronger; more advanced IT backbone to better serve Veterans with a focus on Managing Data, Migrating to the Cloud, Improving Cybersecurity, Digitizing Business Processes, and Decommissioning Legacy Systems. OIT's five modernization priorities are built on transformation. They facilitate a modern IT infrastructure that supports OIT's vision of becoming a world-class organization that provides a seamless, unified Veteran experience through the delivery of state-of-the-art technology.

The Path Forward

We are plotting a path forward for a modern VA that seamlessly connects Veterans with the care, benefits, and services they have earned. In OIT, we are committed to investing in new and emerging IT solutions such as artificial intelligence, robotics, and self-service tools that revolutionize the way Veterans and VA employees interact with our digital framework. This commitment enables VA to continue to provide high quality, efficient care, and services that keep up with the latest technology solutions and standards of care. The future of VA's IT modernization is rooted in eight of our key initiatives: EHRM, enterprise-wide API Management Platform, Financial Management Business Transformation, cybersecurity, scheduling enhancements, telehealth expansion, legacy system modernization, and data center consolidation.

First and foremost is our EHRM initiative. On June 5, 2017, Secretary Shulkin announced his decision to adopt the same Electronic Health Records (EHR) technology as DoD. This transformation is about improving VA services and significantly enhancing the coordination of care for Veterans who receive medical care not only from VA, but DoD and our community partners. We have a tremendous opportunity for the future

with EHRM to build transparency with Veterans and their care providers, expand the use of data, and increase our ability to communicate and collaborate with DoD and community care providers. In addition to improving patient care, a single, seamless EHR environment will result in a more efficient use of VA resources, particularly as it relates to health care providers. This new EHR system will enable VA to keep pace with the improvements in health IT and cyber security, which the current system, VistA, is unable to do. Moreover, the acquisition of the same solution as DoD, along with the added support of joint interagency governance and support from national EHR leadership including VA partners in industry, government, academic affiliates, and integrated health care organizations, will enable VA to meaningfully advance the goal of providing a single longitudinal patient record that will capture all of a Servicemember's active duty and Veteran health care experiences. It will enable seamless care between the Departments without the additional step of exchanging and reconciling data between two systems that are not integrated and operate in separate environments. To that end, the Secretary has insisted on high levels of interoperability and data accessibility with our commercial health partners in addition to the interoperability with DoD. Collectively, this will result in better service to Veterans since transitioning Servicemembers will have their medical records made available to VA without any intervention.

Our second initiative supports VA's commitment to leverage our community partners and innovative technologies to give Veterans a digital experience in line with what they receive from the private sector through APIs. VA's strategic open API program called Lighthouse that adopts an outside-in, value-to-business driven approach to create APIs that are managed as products to be consumed by developers internal and external to VA. Such an approach serves as a change catalyst, which will allow VA to decouple systems and continue to leverage its investment in various digital assets, support application rationalization, and allow it to absorb new, commercial SaaS to replace homegrown, outdated systems. This strategy calls for a clearly defined operating model for managing the complete life cycle of APIs and will include the planning, design, implementation, publication, maintenance, and retirement of APIs as well the operation of the API Gateway platform on a VA private cloud.

The API Gateway leverages FHIR so as to enable enhanced data interoperability between both internal and external systems. API enabled and FHIR-based solutions are easier for developers to implement as it makes use of modern web standards and RESTful architectures with more easily understood specifications. By liberating data and enhancing interoperability with FHIR, VA will be able to shift ownership of the data to Veterans and make that data more readily available for whom it is necessary. Additionally, these resources will allow for more powerful solutions to be developed which will allow for a more seamless patient and provider experience.

We released our developer sandbox in beta 2 weeks ago. We are looking for a small, initial-user group to join our developer community to make sure we follow industry best practices around tools, documentation, governance, and support workflows. As this community grows and VA releases more APIs, Lighthouse will serve as the "front

door" to VA's vast data stores—giving developers access to standardized data sets they need to build mobile and web apps for our Veterans.

As part of VA's commitment to promoting interoperability and standardized data sharing through Lighthouse, Secretary Shulkin announced VA's Open API Pledge, which reaffirms VA's commitment to giving developers access to our systems through standards-based APIs so that they can build Veteran and clinician-designated applications. In exchange, we are asking health care providers to sign a pledge to work with VA to accelerate the mapping of health data to industry standards, including the current and future versions of FHIR.

Our third initiative supports VA's back-end systems and reduces our reliance on outdated legacy systems, so our clinicians and employees have the modern tools and IT support they need. VA's Financial Management Business Transformation effort is currently underway and will positively impact the delivery of all health and benefits by standardizing and improving accounting and acquisition activities across VA's enterprise. VA has an urgent need to address multiple legacy platforms used today in our finance and accounting mission critical functions. We are working to adopt and implement a commercial, cloud-hosted integrated financial and acquisitions system. This transformation effort will increase the transparency, accuracy, timeliness, and reliability of financial information. The result will be improved fiscal accountability to American taxpayers and improved care and services to our Veterans as well as transforming the Department from numerous stovepipe legacy systems to a proven, flexible, shared service business transaction environment.

Our fourth initiative focuses on bolstering our enterprise cybersecurity framework to proactively respond to emerging data threats and the evolving cybersecurity landscape. VA's Enterprise Cybersecurity Strategy will ensure that Veteran data are secure, available, and safe from cyber threats. Safeguarding Veteran information and VA data is essential to providing quality health care, benefits, and services to our Nation's Veterans.

Our fifth initiative extends to modernizing and enhancing the Department's scheduling systems. As a patient who receives treatment at both the Washington, DC, and Baltimore VA Medical Centers, enhanced scheduling is something I am very passionate about. We are launching new digital tools that enable Veterans to schedule appointments online, use mobile applications to manage prescriptions, and participate in video conferences with their care providers as needed. We are also investing in solutions that give our providers a more seamless experience with the back-end scheduling tools they need to serve our Veterans. We have made strides in our scheduling tools, but we still have a long way to go. We now have VistA Scheduling Enhancement (VSE) upgrades fully implemented in 158 of 160 sites improving the interface for the schedulers so they easily view appointment times and reduce scheduling errors. Any person can now conduct their Scheduling activities at those sites using VSE. Some sites have greater utilization than others based on the level of training of users per site, which is increasing daily. We have seen online scheduling

increase 5 times due to recent improvements; this capability is currently in place at more than 100 sites. The Medical Appointment Scheduling System is being piloted in Columbus, Ohio, and the Faster Care for Veterans Act test installs have been successfully completed in Minneapolis, Minnesota; Salt Lake City, Utah; and Bedford, Massachusetts. Last year, the Secretary launched a new access and quality tool, known as "Access to Care." This web-based site was developed for Veterans and their families to see in real time the wait times at local VA facilities, VA hospital ratings, and comparisons with private hospitals in their area. This information empowers Veterans to choose the time and place they receive their care. Not only will this website take in and process complex data, but it will make the data transparent to Veterans. We will continue improving transparency via the Access to Care site as we receive feedback from Veterans, employees, Veterans Service Organizations, and Congress.

In addition to scheduling enhancements, VA and OIT are making strides in our telehealth programs. We are expanding telehealth capabilities with hubs around the country to better service Veterans who live in rural communities or have challenges accessing VA medical centers due to their mobility. More Veterans have access to tele-mental, tele-urgent, and tele-specialty care. On March 6, 2018, the Secretary announced VA's plan to launch a nationwide telehealth program to help Veterans dealing with post-traumatic stress disorder (PTSD). The pilot program will connect 12 community-based outpatient clinics (CBOC) across the Nation with Veterans in need of treatment for PTSD. This program will help greater numbers of Veterans living in rural areas and will save them time and effort to travel to a VA facility that is far from their homes.

Another significant VA and OIT initiative is Legacy Systems Modernization. We are moving critical functions from outdated and difficult to sustain platforms into more modern systems that operate at lower maintenance costs. Our planned IT investments prioritize the development of replacements for specific mission critical legacy systems, such as the Benefits Delivery Network, as well as operations and maintenance of all VA IT infrastructures essential to deliver medical care and benefits to Veterans. Investments in IT will also support efforts and initiatives that are directly Veteran-facing, such as mental health applications to support suicide prevention, modifications of multiple programs to accommodate special requirements of the community care program, Veteran self-service applications (Navigator concept), education claims processing integration consolidation, and benefit claim appeals modernization.

OIT continues its Data Center Consolidation effort to merge and close data centers at VA facilities nation-wide. During FY 2017 the team closed 24 data centers. The team plans to close another 91 by the end of FY 2018. The benefits of the Data Center Consolidation effort include increased system security, reliability, and efficiency; enhanced cybersecurity; and the opportunity to introduce innovative and cost-saving technological advances to VA systems. These improvements will allow VA employees to spend less time managing the infrastructure and more time on customer-focused activities that better serve Veterans. As OIT continues to make progress in data center consolidation, VA will remain a government leader in compliance with FITARA.

We are on an ambitious journey to become the number one customer service agency within the Federal Government. By investing in innovative solutions—from technology to new ideas—we are on the right trajectory to advance toward our modernization goals and to make VA a greater choice for all Veterans.

CONCLUSION

Thank you again for the opportunity to appear before you today to address the status and progress that the VA OIT is making towards its deployment of the CDM Program and our IT modernization efforts. Throughout this modernization, 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 look forward to answering your questions.

Mr. Scott R. Blackburn

Executive in Charge

Mr. Blackburn was designated to serve as the Executive in Charge for the Office of Information and Technology on October 2, 2017 by VA Secretary David J Shulkin, M.D.

Mr. Blackburn was appointed Department of Veterans Affairs Interim Deputy Secretary on February 26, 2017.

Mr. Blackburn joined VA in November 2014, serving first as Senior Advisor to the Secretary on Transformation and, then, as Interim Executive Director of the MyVA Task Force.

That means he's helped conceive, design, launch, manage, and now, lead VA's ambitious journey to be a world-class service provider and the No. 1 customer-service agency in the Federal government.

Prior to VA, Mr. Blackburn was a consultant at McKinsey & Company, where he helped transform cultures of large, often bureaucratic, Fortune 500 companies. He was named partner in 2011.

Mr. Blackburn hails from a family with a strong tradition of military service. All four of his siblings are Veterans, and he served in the Army from 1999 to 2003 as an Armor and Signals Corps officer. Mr. Blackburn's a Veteran of Operation Enduring Freedom and Operation Anaconda in Afghanistan.

Medically discharged after a non-combat-related back injury in Kuwait, Mr. Blackburn's a beneficiary of VA's Vocational Rehabilitation Program that facilitated a smooth transition from uniform to university. In 2005, Mr. Blackburn graduated from Harvard Business School

Born in Concord, Massachusetts, he's particularly proud that he was raised in the coastal town of Scituate, popularly known as the Irish Riviera.