AMENDED PASSBACK

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

December 7, 2017

Good morning, 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 (OIT) is making towards its transformation efforts with an emphasis on Information Technology (IT) modernization; Enterprise Cybersecurity Strategy; Federal Information Security Modernization Act (FISMA), and Federal Information Technology Acquisition Reform Act (FITARA) compliance; and the Electronic Health Record Modernization (EHRM) initiative. I am pleased to be accompanied today by Mr. Bill James, Deputy Assistant Secretary for the Enterprise Program Management Office (EPMO), Mr. Dominic Cussatt, Chief Information Security Officer, Mr. John Short, Executive Director for Information Technology Systems Modernization, and Mr. John Windom, Program Executive for Electronic Health Record Modernization.

The health, safety, and welfare of our Veterans are among our highest national priorities. As one of five siblings who are Veterans or still serving in uniform and who are all at least fourth generation U.S. military Veterans, I take personal pride every day in fulfilling VA's sacred mission, which was passed down to us by President Abraham Lincoln more than 150 years ago, to care for those who "have borne the battle" and for their families and survivors. VA, and OIT, is in the middle of a turnaround. Trust was broken in 2014; helping re-earn that trust is why I left the private sector to join VA in November 2014. When we started a quarterly survey to measure Veteran trust of VA 2 years ago, only 47 percent of Veterans said they trust VA to fulfill our Nation's

commitment to Veterans. Today, that number is 69 percent, and we have seen an uptick in each of the last seven quarters. OIT has played a major role in that improvement and will only play an even more important role as we continue to modernize and regain the trust of all Veterans. We are proud of our progress, but we clearly still have a lot of work to do.

This is not the first time OIT leadership has appeared before the Subcommittee. On March 16, 2016, my predecessor, Ms. LaVerne Council, discussed the progress OIT was making to better serve our business partners, our Veterans, and examined VA's implementation of FISMA and FITARA, as well as specific information technology (IT) investments. My testimony will build on this, covering a number of the subject areas raised previously and will provide you with a glimpse into the significant progress we have made since that time.

IT MODERNIZATION

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 like 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 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. In OIT, we are committed to the following efforts, which align with the Secretary's initiatives to provide greater choice and transparency for Veterans, modernize systems, focus resources more effective and efficiently, improve timeliness of services, and prevent Veteran suicides.

First and foremost is our Electronic Health Record (EHR) Modernization effort, which is a major White House initiative, and has received a fair amount of media and Congressional interest. In arriving at his decision on our Next-Generation EHR for VA, the Secretary reviewed numerous studies, reports, and commissions on this topic,

including the recent Commission on Care report. He also spent considerable time talking to clinicians and consulting with Chief Executive Officers from leading health systems to solicit their own thoughts.

This led the Secretary to announce that VA will begin to work toward a single common solution by adopting a new EHR system, using the same state-of-the-art solution currently being deployed by the Department of Defense (DoD). The selection of a new EHR strategy is a major step forward for VA and is a critical component of our strategic commitments. We hope to very soon finalize and sign a contract with Cerner Corporation to begin this work with our first pilot sites located in Washington State, leveraging the work and lessons learned from DoD and Cerner. With regard to the standardization of VistA over the past 18 months, the clinically validated data extraction work was conducted by the BISL CDW team, and the data migration planning started in August 2016. These efforts will help make the Cerner rollout in 18 months more successful.

As we proceed in a thoughtful and deliberate manner, our teams will incorporate critical lessons and experiences learned from the visionaries and users of our legacy VistA system and DoD's lessons learned from deploying the same Cerner solution to contribute to building the most advanced, integrated EHR in the Nation. This path forward will make a big difference for Veterans everywhere and will provide VA clinicians modern tools to deliver the seamless care Veterans deserve. Having an EHR that can follow our Veterans during their health and treatment is one of the most important things we can do to ensure their safety, health, and general well-being. The adoption of the same system between VA and DoD will allow for all patient data to reside in a common system, so there will be a seamless link between the Departments without the manual or electronic exchange of information. A Veteran will now be able to have a single common system from the time of enlistment or commission throughout their life, with one single lifetime record. There will never be a need to go back and forth between Departments and say, "records are not there for me", or "my doctor is not able to have input into what the DoD is doing." This is because VA and DoD's interoperable

EHR system is based on a single instance and database, so all DoD records will be available to VA as soon as they are available to DoD.

Today, VA and DoD share more medical information than any two health care organizations in the country. We have developed and deployed, in close collaboration with DoD, the Joint Legacy Viewer (JLV) to enable this data sharing capability. The JLV is available to all clinicians in every VA facility and is a web-based user interface that provides clinicians with an intuitive display of DoD and VA health care data on a single screen. As of November 1, 2017, the latest data identified 89,623 DoD and 332,586 VA users. Between May 2013 and October 2017, almost 8 million medical records have been viewed through JLV. The outcomes of VA and DoD joint development on JLV is a clear demonstration of the business outcomes the two agencies can deliver through deep collaboration and integration. While JLV is very valuable, the proposed new EHR will add and improve the capabilities we have today in JLV. This will allow VA and DoD to build on the success of JLV by having a single instance of a Veterans record.

A second commitment involves modernizing the Benefits Delivery Network (BDN). A 50-plus year old COBOL-based legacy system, BDN is the primary database and payment system for VA's education benefit programs and is something that supports Veterans every day. Modernizing the BDN will ensure that Veterans Benefits Administration (VBA)-wide financial payment and processing of 4 million checks each month remains feasible and those Veterans continue to receive the benefits they have earned in a timely manner. BDN has generally had a successful payment history for over 40 years.

A third commitment is our continuing effort to Improve Enterprise Cybersecurity. VA's Enterprise Cybersecurity Strategy will ensure that Veteran data is 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. More specific details associated with our Enterprise Cybersecurity Strategy can be found later in this testimony.

Our fourth commitment extends to modernizing the Department's scheduling systems – which as a patient who receives treatment at the Washington DC VA Medical Center, Orange Clinic - is something I am very passionate about. This is an area where we have made improvements but still have a long way to go. We now have VistA Scheduling Enhancement (VSE) upgrades fully implemented in 130 of 158 sites, improving the interface for the schedulers so they easily view appointment times and reduce scheduling errors. Just in the past month, we have seen online scheduling increase 5 times due to recent improvements (4,541 appointments scheduled online between 11/09/17-11/30/17);this capability is currently in place at more than 100 sites. Medical Appointment Scheduling System (MASS) in 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. As Cerner deploys to each site, it will be converted to Cerner's resource based Scheduling System. Earlier this 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 and VA hospital ratings in comparison with private hospitals in their area. This information empowers Veterans to choose the time and place they receive their care. Not only will this web-site take in and process complex data, but it will make these 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 software, we are making strides with our technology and business partners. We completed a proof of concept for the Digital Health Platform, now called the Digital Veteran Platform, or DVP, marking an entirely new approach to health care. DVP is a revolutionary concept in health care information technology management that enables interoperability among systems much more efficiently than traditional system integration efforts. DVP will allow commercial application developers to create solutions that connect internal and external care providers to support comprehensive seamless Veteran care across organizational boundaries and clinical

systems. Further, DVP will create an open, accessible platform that can be used not only for Veterans' care, but also for advanced knowledge sharing, clinical decision support, technical expertise and process interoperability with organizations through the US care delivery system by simplifying access to the largest data set of clinical data anywhere. This will accelerate the discovery and development of new clinical pathways for the benefit of the Veterans and community at large.

Another significant OIT commitment is modernizing the legacy Financial Management System to standardize and improve accounting and acquisition activities across the VA enterprise. VA has a clear and 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.

ENTERPRISE CYBERSECURITY STRATEGY (ECSS)

VA, our core constituents, and our external partners are subject to a wide variety 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. The purpose of the Enterprise Cyber Security Strategy, also known as ECSS, is to guide agency-wide cybersecurity planning and risk-based decision making. ECSS directs VA leadership to act as cybersecurity resource stewards to identify and articulate requirements, standards, and opportunities for transformative cybersecurity improvements.

Within OIT, we are committed to protecting Veteran information, VA data, and limiting access to only those with the proper authority. This commitment requires us to think agency-wide about security holistically. ECSS promotes collaboration, enables data protection, and provides resiliency in the face of a broad spectrum of threats through the realization of the following five strategic cybersecurity goals:

- **Veteran Information and VA Data are Protected:** Data protection is an essential VA function that involves people, processes, and technology. VA must identify its high-value assets (HVA); understand its business processes and system interactions so that security and privacy protections can be applied commensurate with risk and enhance awareness of safe information handling practices so that the VA workforce, Veterans, and partners are equipped to help protect VA data and Veteran information.
- **VA's Cyberspace Ecosystem is Resilient to Threats:** VA needs to maintain critical functions in the face of inevitable breaches. While defense in depth remains essential, we as an organization must also be resilient. Implementing the appropriate policies, procedures, and technologies provides VA with the ability to maintain continuity of operations both during and after a cyber event, as well as evolving VA's resiliency to better adapt to advanced cyber threats.
- **VA Information Systems and Infrastructure are Protected:** VA identifies and strengthens its mission critical systems and infrastructure, modernizes IT, and employs an integrated, resilient architecture. VA is also committed to leveraging cloud and Federal shared services. VA not only integrates cybersecurity protections into VA information systems and networks but also verifies that business associates are appropriately implementing protections within their systems.
- **A Secure Operational Environment Supports Effective Operations:** For VA to operate effectively in the cybersecurity domain, a secure operational environment is necessary. Such an environment is realized through efficient, agile acquisitions that help VA keep pace with evolving cyber threats and technological innovations, operates transparently and, to the extent possible, seamlessly and is enabled by integration of information security capabilities and outcomes across enterprise governance, business operations, and technology architecture frameworks.
- **VA Recruits, Develops, and Retains a Talented Cybersecurity and Privacy Workforce:** Strong cybersecurity capabilities require a cybersecurity workforce

that is agile, multifunctional, dynamic, and flexible to adapt to an ever-changing threat environment. VA's workforce planning capability and framework provide VA the data it needs to make fact-based decisions on cyber and privacy workforce recruitment, development, and retention.

To achieve this end, our Office of Information Security (OIS) manages cybersecurity risk through VA's Enterprise Cybersecurity Strategy Program, or 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 include the reinforcement of VA's strategic goals and objectives that inform cybersecurity behaviors at VA. Our principles include, but are not limited to, patient safety, holistic risk management, adaptive defense and cyber resiliency, security, and privacy integration, shared services, and IT modernization.

With the establishment of the ECSP, we are embarking on a change in mindset of how to manage cyber risk. Through the 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 (NIST) Cybersecurity Framework (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.

As part of our Enterprise Cybersecurity Strategy Team (ECST), we have recently focused on the following:

- Plans of Action created in response to the fiscal year (FY) 2015 Office of Inspector General (OIG) FISMA audit.

- 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.

Recent OIS Accomplishments

Through ECST, we have been able to achieve various program, capability, and policy milestones on the path to further advancing the VA cybersecurity program:

From a programmatic perspective:

a. We have established a plan to transition from the ECST to ECSP to enable proactive cyber risk management through the prioritization of cybersecurity projects and alignment to the NIST CSF.
b. We formally established an Information Security Continuous Monitoring (ISCM) Strategy, as well as an Integrated Project Team (IPT) Charter for management oversight, implementation, and operation of the program.

With regard to capability milestones:

a. We continue to develop a risk-scoring model, which is designed to advance VA's implementation of the NIST Risk Management Framework (RMF) and assist with prioritizing risk across security and privacy control families in support of proactive cybersecurity risk management.
b. Since the middle of 2015, we have reduced the number of elevated privileged user accounts for employees and contractors by 96 percent.

c. We have developed a new end-user driven site map and updated design to support adoption of the VA Knowledge Service as the single authoritative source of VA control policy and implementation guidance.
d. Within the Knowledge Service, we have also developed an interactive Security Controls Explorer to provide OIT stakeholders (e.g., System Owners, Information Security Officers) with implementation guidance for applying the NIST RMF to VA information systems.
e. We created a process for VA to consistently analyze planned software implementations against the One-VA Technical Reference Model, used as a technology roadmap and tool for supporting OIT, prior to project initiation.
f. We implemented a process to annually test contingency plans and failover capabilities for applications and general support systems based on system/site categorization levels.
g. We updated the Assessment and Authorization process by focusing on increasing system owner accountability for systems nearing Authority to Operate (ATO) expiration.
h. We also created an organizational library of security incidents with root cause analyses and corrective actions for educational/response references for future incidents.

With respect to revising policies and guidelines:

a. We have developed a cloud security framework that aligns with the NIST CSF.
b. We have also instituted a new firewall policy to cover new technologies in coordination with the Office of Cybersecurity Policy and Compliance.
c. We have published Directive and Handbook 6513, Secure External Connections, which governs the process for managing and continuously monitoring VA connections.

FISMA AND FITARA COMPLIANCE

FISMA Update

Through OIS, we currently manage a Cybersecurity Policy and Reporting Requirements Matrix which tracks FISMA submissions by VA. Through this matrix, we are able to organize and track cybersecurity policies, public laws, and NIST Special Publications guidance, Federal Information Processing Standards, Internal/Interagency Reports. The matrix also tracks VA's recurring reporting requirements that are submitted to Government-wide authorities such as Congress, the Department of Homeland Security (DHS), and OMB, and is updated when new rules, regulations, and recommendations are published.

VA is able to leverage the Cybersecurity Policy and Reporting Requirements Matrix to follow FISMA guidelines and laws in accordance with the following:

- OMB Memorandum M-17-05, Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements;
- OMB Memorandum M-17-25, Reporting Guidance on the Executive Order of Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure;
- The recent Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure;
- The Federal Information Security Modernization Act, or FISMA, of 2014;
- The E-Government Act of 2002;
- The FY 2017 FISMA Chief Information Officer (CIO) Metrics (October 2016); and
- The FY 2017 FISMA OIG Metrics (April 2017).

As of October 31, 2017, we have reported our FISMA Maturity Model responses to DHS, including Information Security Continuous Monitoring (ISCM), Risk Management, Configuration Management, Contingency Planning, Identity and Access Management, Incident Response, and Security Training.

In response to the 2017 OIG FISMA Audit, OIT is currently conducting an analysis of the FY 2017 audit findings in order to determine the appropriate remediation measure to take. In addition, OIS has mapped our recent FY 2017 OIG findings to NIST security and privacy controls in order to identify the controls which were commonly aligned to findings within the audit. By this mapping exercise, OIS will be able to discern the controls that require more attention and prioritize future projects based on this information. In preparation for future audit cycles, OIS is planning to develop detailed control implementation guidance for high-risk controls, providing the field with the knowledge base they will need to successful execute controls on a day-to-day basis. As the control implementation guidance is developed, it will be incorporated into the VA RMF Knowledge Service (KS); the KS will serve as the single authoritative source of VA control policy and implementation guidance.

FITARA Progress

For the third consecutive rating period, VA received a B+ grade from the House Committee on Oversight and Government Reform FITARA scorecard. While we are pleased by our score, we are not satisfied and are seeking ways to improve upon that grade. Our goal is to raise the score to an "A," and we are taking steps to achieve this milestone. One of those steps is the establishment of an OIT-based Strategic Sourcing division to ensure FITARA compliance for all IT acquisitions. Strategic Sourcing practices will improve speed to market, compliance and quality for IT solutions, provide VA with access to industry innovation, and empower employees who have the deepest understanding of the work to deliver the best solution, at the best value, to the Veteran.

The IT Operations and Services (ITOPS) division within OIT supported acquisition and asset management improvements that directly tie to the A grade that VA

received in Software Inventory, a subcategory in the scorecard. In addition, ITOPS continues its Data Center Consolidation effort to merge and close data centers at VA facilities throughout the country in accordance with OMB's Data Center Optimization Initiative memorandum, which mandated a freeze on the development of new data centers and a consolidation of the rest. This year, the team closed 23 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 build the Strategic Sourcing division and its capabilities, and continues to make progress in data center consolidation, VA will remain a Government leader in compliance with this legislation and VA's FITARA score will continue to improve.

ELECTRONIC HEALTH RECORD MODERNIZATION INITIATIVE

On June 5, 2017, Secretary Shulkin announced his decision to adopt the same EHR system as DoD, which at its core 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. Having a Veteran's complete and accurate health record in a single common EHR system is critical to that care and to patient safety. This new EHR system will enable VA to keep pace with the improvements in health information technology and cyber security which the current system, VistA, is unable to do. In addition, the new EHR will support the critical need for VA to effectively and efficiently share patient data with DoD and community partners.

With Congress' urging, VA and DoD have been working together for over 17 years on EHR issues. While we have established some interoperability between VA

and DoD for key aspects of the health record, seamless care is fundamentally constrained by ever-changing information on sharing standards, separate chains of command, complex governance, and a host of related complexities requiring constant lifecycle maintenance resulting from separate implementation schedules, program offices, and funding appropriation.

Despite previous efforts, we still do not have the ability to trade information to seamlessly execute a shared plan of care for our Veteran patients. Without improved and consistently implemented national interoperability standards, VA and DoD will continue to face significant challenges in providing the highest quality of care for our Veterans.

For these reasons, the Secretary decided that VA would adopt the same EHR system as DoD, which at its core consists of Cerner's Millennium EHR. Adopting Cerner's EHR system, which the Secretary believes is in the Veterans' and the public's interest, will ultimately result in all patient data residing in one common system. It will enable seamless care between the Departments without the current manual and electronic exchange and reconciliation of data between two separate systems. It will also result in better service to our Veterans because transitioning Service members will have their medical records at VA on day one.

Replacing VistA is a Must

Continuing to maintain VistA is more costly in the long-run and will not meet full interoperability. To bring VistA up to where it needs to be is our most expensive option. VA would have to spend roughly $19 billion over 10 years to upgrade and maintain VistA to industry standards, and this still would not provide all the needed enhancements and upgrades and interoperability with DoD. In addition, VA currently has fewer programmers than it did when VistA was designed and will be much more expensive to maintain on an ongoing basis as compared to a more modern Commercial

Off-the-Shelf (COTS) solution. VistA is in many ways like the car that we love and don't want to trade in, though it is now costing us way too much money to maintain.

The current VistA system is made up of 130 instances of the VistA EHR. Even if VA were to make the required upgrades to VistA, it still would not be able to deliver all the capabilities that the new Cerner EHR system will include, specifically a single common system to provide seamless care with DoD, and improved integrated interoperability with community providers via health information exchanges.

VA Will Leverage DoD's Efforts

Throughout our negotiations with Cerner, VA has been able to leverage lessons learned from DoD. VA is approximately three times the size of DoD's health care system. VA has 2.5 times more facilities (1,675 vs. 665); 3.7 times more interfaces (102 vs. 27); and triple the licensed users. In addition, VA's patient population will necessitate the purchase of a greater number of services and capability requirements, including greater health care interoperability and information exchange nationally, which will improve interoperability with community providers.

Efficiencies as a Result of EHR Modernization

VA will find considerable savings/efficiencies across our existing systems. Transition solutions for nearly all (138 of 143) VistA modules have been identified; the majority of which will be replaced directly by Cerner as part of our EHR modernization effort. The Cerner solution and VistA EHR will be operating simultaneously for an extended period of time with the appropriate decommissioning plan of VistA to ensure no disruption of services to our Veterans during the transition of capabilities from VistA to our modernized EHR.

The VA EHRM Team is working hand-in-hand with their DoD counterparts to ensure that seamless care and information exchange objectives are fully realized.

Efforts include the exchange of lessons learned, alignment of EHRM deployment schedules to support early interoperability successes and the establishment of an interagency governance board to promote configuration management control and long-term adherence to interoperability objectives.

Adoption of Cybersecurity Enhancements

Within the breadth of VA's migration to a new EHR system, we are actively assessing the need for VA to adopt significant cybersecurity enhancements, and we intend to leverage the architecture, tools, and processes that have already been put in place to protect DoD data, to include both physical and virtual separation from commercial clients. We are coordinating with DoD on near-term activities regarding agency reciprocity for the EHR system ATO, EHR data, and a VA-DoD reciprocity task force. VA has undertaken activities that will further align VA RMF and Assessment and Authorization processes to current DoD practices. These activities include but are not limited to the following:

- RMF collaboration, to include the sharing and analysis of: security and privacy controls, ATO documentation, and security artifacts;
- Drafting an ATO reciprocity memo to include the EHR system and other ancillary partnership efforts between VA and DoD;
- Collaboration with DoD on the EHR architecture and risk tolerance levels;
- Acquisition of the eMASS Governance, Risk Management, and Compliance tool, of which DoD currently uses; and
- Establishment of the VA RMF Knowledge Service (KS) similar to DoD. The KS will contain security policies and guidance, as well as new NIST security control implementation and assessment procedures.

Oversight and Transparency

VA will provide full transparency in this project, including an Initial Operating Capability milestone and other decision points prior to full deployment. We would also like to request establishment of a separate new appropriation account for EHRM costs. A separate account would allow all EHRM costs to be captured in one place, provide full transparency of and accountability for resources, and enhance EHRM implementation. Finally, this is being managed differently than past efforts. First, this is a Secretary-Level initiative, with the Deputy Secretary overseeing the new governance structure, which includes OIT and VHA. Additionally, we are using a buy vs. build strategy to implement proven technology from an industry leader. Finally, we are leveraging lessons-learned from DoD as well as private sector expertise in a way that has not been done before.

CONCLUSION

Mr. Chairman and Madam Ranking Member, this concludes my testimony. Thank you again for the opportunity to discuss with you today the progress that the VA OIT is making towards its transformation efforts. 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 look forward to answering your questions.