STATEMENT OF PAUL CUNNINGHAM
CHIEF INFORMATION SECURITY OFFICER
OFFICE OF INFORMATION SECURITY
OFFICE OF INFORMATION AND TECHNOLOGY
DEPARTMENT OF VETERANS AFFAIRS
BEFORE THE
HOUSE COMMITTEE ON VETERAN'S AFFAIRS
SUBCOMMITTEE ON TECHNOLOGY MODERNIZATION

NOVEMBER 14, 2019

Good morning Madam Chair Lee, Ranking Member Banks, and distinguished Members of the Subcommittee. Thank you for the opportunity to testify today in support of the Department of Veterans Affairs (VA) cybersecurity initiatives to protect Veterans' and VA employees' sensitive data. I am accompanied today by Gary Stevens, Deputy Chief Information Security Officer, Executive Director for Information Security Policy and Strategy, Office of Information and Technology (OIT), Mr. Andrew Centineo, Executive Director, Procurement and Logistics, Veteran Health Administration (VHA) Procurement and Logistics Office, and Ms. Luwanda Jones, Deputy Chief Information Officer, Strategic Sourcing, OIT.

I want to begin by thanking Congress, and specifically this Subcommittee, for your continued support and shared commitment to the success of VA cybersecurity program. VA's mission of improving health care delivery to our Nation's Veterans and those who care for them while being responsible to safeguard their private information is conducted because of your unwavering support.

Introduction

The Department of Veterans Affairs (VA) Office of Information and Technology (OIT) has the great responsibility of safeguarding Veteran information and VA data, ensuring VA's networks and infrastructure are resilient to threats, and maintaining a secure operational environment that supports business needs and mission outcomes. OIT's Office of Information Security (OIS) is the primary office that carries out these responsibilities. OIS' mission is to protect the Personally-Identifiable Information (PII)

and Protected-Health Information (PHI) of Veterans, their families, and VA employees, as well as VA information systems and infrastructure. Security and privacy are integral to the Veteran experience. For this reason, VA believes that exceptional service to our Veterans can only be achieved in a secure digital environment. This belief guides a cybersecurity strategy that rises to meet the highest standards while focused on the protection of the Veteran.

VA has a complex cybersecurity environment, with over 1.6 million connected devices across approximately 2,500 facilities ranging from offices to data centers to VA hospitals, benefits regional offices, and beyond. Additionally, Secretary Robert Wilkie has outlined a Department-wide modernization strategy to transform and enhance how VA serves Veterans. VA is transforming the Veteran experience, providing them increased access to services and information. Migrating from legacy systems and allowing Veterans to access this information requires VA to further extend its digital footprint, introduce new technologies, and increase interoperability and data sharing. However, these improvements also introduce unique cybersecurity, privacy, and third-party risks. VA's cybersecurity strategy and posture aim to address these risks while enabling and improving business processes and shifting VA to a proactive stance in an ever-changing cyber landscape.

VA's cybersecurity posture consists of a holistic and robust set of strategies, programs, and capabilities. VA's 2019 Enterprise Cybersecurity and Privacy Strategy (ECPS), borne out of its Enterprise Cybersecurity and Privacy Program (ECSP), articulates the Department's current cybersecurity strategy and future cyber and privacy goals. These goals include enhanced risk management, secure interoperability, exceptional customer service, secure and resilient business processes, and a strong cyber and privacy workforce and culture. The Program, which was developed in 2015 and fully implemented in 2017, governs the Strategy and shifts VA to a proactive cybersecurity posture with programs and capabilities including the following:

- Supply Chain Risk Management (SCRM);
- Governance, Risk Management, and Compliance (GRC) tool;

- Information Security Continuous Monitoring (ISCM);
- Continuous Diagnostics and Mitigation (CDM); and
- Cybersecurity Operations Center (CSOC).

FY 2019 Enterprise Cybersecurity and Privacy Strategy (ECPS)

For Fiscal Year (FY) 2019, VA updated its ECPS to align with its Department-wide modernization strategy and to further mature its cybersecurity posture. The updated ECPS will adopt industry and Government best practices, account for changes in the cybersecurity landscape, and build a proactive and forward-looking cybersecurity posture. VA's updated ECPS consists of the following five goals: (1) Enhance enterprise cybersecurity and privacy risk management; (2) Ensure secure interoperability both within and outside VA; (3) Deliver exceptional customer service; (4) Enable secure and resilient business operations; and (5) Cultivate a VA cybersecurity and privacy workforce and culture. Together, they strengthen cybersecurity at VA while also improving business processes, and by extension, the service VA provides to Veterans.

(1) To enhance enterprise cybersecurity and privacy risk management, VA will emphasize cybersecurity and privacy in enterprise-wide risk management processes. VA has implemented the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) to manage the Department's cybersecurity risk at three organizational levels: information system, mission area/business process, and organization. The VA is leveraging cybersecurity best practices, from NIST, to address threats to medical devices, supply chain processes, financial services, and sources of protected Veteran information. Additionally, the framework drives VA decisions about cybersecurity and privacy investments.

(2) To ensure secure interoperability both within and outside the Department, VA must protect data regardless of location. Access methods must be secure and flexible, protecting data while enabling VA business processes. VA is

leveraging shared security and privacy capabilities and collaborating with Federal and commercial partners and third-party providers to meet and enforce Federal security and privacy requirements. For Veterans, interoperability means streamlined access to data and services – but not at the expense of security and privacy.

(3) In pursuit of its permanent goal to deliver exceptional customer service, VA is integrating its cybersecurity policies and standards into business processes. With this integration approach, security and privacy are an enabler, not a barrier, to efficient business processes, facilitating Department-wide adoption of a rigorous cybersecurity posture.

(4) To enable secure and resilient business operations, VA is improving cyber hygiene across the Department. Good cyber hygiene limits threat exposure, accelerates adoption of protective cyber technologies, and enhances cross-organizational incident response processes.

(5) VA continually aims to cultivate a VA cybersecurity and privacy workforce and culture. VA is recruiting, training, and retaining a talented cyber and privacy workforce through its cyber retention pay and benefits, career progression tools, and training opportunities. VA is renaming Development Operations (DevOps) – a program office established this year to shift VA to an Agile development mindset – to Development Security Operations (DevSecOps). This change also reflects and embodies VA's security-first mindset as a cyber-conscious organization because protecting Veterans' information is not only a technical concern but a human and customer service issue.

VA plans to execute its updated ECPS by aligning the strategy with NIST RMF and Cybersecurity framework (CSF) policies and standards, as well as with internal stakeholder business processes. VA ensures enterprise-wide awareness and adoption of the strategy by aligning cyber policies and activities with business requirements and processes. With a robust cybersecurity posture baked into business processes, the

Department can be sure that security and privacy are the baseline for every service provided to Veterans.

Enterprise Cybersecurity Program (ECSP)

VA's ECPS is governed by the ECSP, the Department's sanctioned cybersecurity program. VA established ECSP under the authority of an official memorandum issued in April 2018. The memorandum was issued in response to Executive Order (EO) 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. The transition to ECSP marked a shift from reactive to proactive cyber risk management.

ECSP orients VA to adopt a more proactive approach to manage cyber risk by emphasizing cybersecurity projects that are aligned to the NIST CSF. ECSP incorporates leading practices and implements guidance from the NIST CSF to mature VA's cybersecurity posture, capabilities, and culture. ECSP also bolsters VA's proactive cybersecurity posture through the ECSP Prioritization Tool, which allows leadership to prioritize and address the highest-priority cybersecurity concerns. This allows the Department to make informed and defensible decisions about cybersecurity activities.

Finally, ECSP provides mechanisms to support external reporting requirements and maintain an acceptable level of overall cybersecurity risk compliance as required by the Federal Information Security Modernization Act (FISMA) of 2014.

VA's goal is for ECSP to become a sustainable, world-class cybersecurity program that protects VA information systems, and most importantly, Veterans' information. With a successful ECSP guiding VA's cybersecurity activity, Veterans can trust that ease of access does not mean compromised security and privacy.

Supply Chain Risk Management (SCRM)

VA must secure and manage risk related to its supply chain processes. Third party suppliers and external Federal and commercial partners must comply with VA's security and privacy policies to access VA data and information systems.

OIT's Office of Strategic Sourcing (OSS), which modernizes VA's sourcing practices for IT products and services is collaborating with VA's contracting offices to ensure we are ordering from approved resellers of an OEMs products to avoid gray market equipment and we utilize Trade Agreement Act (TAA) compliancy in our contracts. We are also working with VA contracting offices to enforce prohibitive language is referenced in contracts templates preventing contractors and vendors from hiring or teaming with contractors and vendors that have been deemed suspended.

VA also requires that all users of its network meet security requirements specified in each contract. Access is strictly controlled by whether users have a 'need to know' information in the course of their duties. VA assesses cybersecurity risks associated with medical devices during the procurement process. Through OSS and OIS, VA continues to integrate cybersecurity and privacy with procurement, acquisition, and supply chain processes in conjunction with the Technology Acquisition Center (TAC) and other business partners across the Department.

Information Security Continuous Monitoring (ISCM)

VA established the ISCM program to provide Department-wide oversight and governance of ISCM activities according to Department of Homeland Security (DHS) requirements. ISCM consists of a combination of technological, operational, and management capabilities that consistently assess the security posture of VA information systems. These capabilities allow for data-driven risk management rather than compliance-driven risk management. VA is collaborating with DHS to remain in lockstep with Federal statutes, guidance, and updates to the program.

Continuous Diagnostics and Mitigation (CDM)

VA is implementing DHS' CDM program to better safeguard information technology (IT) assets. CDM allows the Department to better grasp its universe of assets, users, and network activity, which in turn allows VA to efficiently and effectively monitor for, identify, and mitigate potential risks.

The CDM program delivers capabilities in five distinct areas: (1) Facilitate continuous monitoring of assets, users, networks, and data through the CDM dashboards; (2) Identify assets on VA's network through Asset Management;

(3) Identify and monitor users on the network through Identity and Access Management; (4) Identify what occurs on the network and how to protect it through Network Security Management; and (5) Manage and protect data on the network through Data Protection Management.

On November 1, 2019, the Department of Veterans Affairs (VA) achieved a major milestone by finishing the implementation of tools for hardware asset discovery giving VA visibility to assets connected to the network. This installation culminated a four-year project that involved personnel from VA and the Department of Homeland Security (DHS) as part of the Continuous Diagnostics and Mitigation (CDM) program administered by DHS. As the VA continues to enhance its CDM capabilities, the Department begun a 30-month effort with DHS called the Request for Service (RFS) 15 which allows VA to enhance our Identity and Access Management (IAM) tools and strategy, allowing VA to better manage users on our network, including those with special access to sensitive systems. Other efforts with DHS and internally at VA are addressing CDM capabilities in order to know what is happening on the network and protecting our data.

Cybersecurity Operations Center (CSOC)

VA's CSOC consistently monitors, reports, and responds to cyber threats and vulnerabilities. The CSOC conducts enterprise network security monitoring for the Department. The CSOC is divided into five sub-programs: Cyber Threat Intelligence, Cyber Technical Services, Cyber Incident Response, Cyber Security Analytics, and Cyber Business Intelligence. Coupled with an improved understanding of IT assets through CDM, consistent monitoring allows the Department to proactively detect, identify, and respond to suspicious activity, mitigating potential cyber risks, and protecting Veterans before their data is ever in danger.

Federal Information Security Modernization Act (FISMA)

FISMA, signed into law in December 2014, defines a framework to protect Government information, operations, and assets against threats. FISMA requires the VA to develop, document, and implement a Department-wide program to secure the information systems that support its unique operations and assets. The law requires annual reviews of information security programs to keep risk at or below specified acceptable levels.

VA submitted its FY 2019 second quarter (Q2) CIO FISMA report to DHS and OMB on April 16, 2019. In the subsequent Risk Management Assessment, VA was evaluated as "Managing Risk" overall, with only the "Respond and Recover" category rated "at risk." Additionally, VA has met seven of the ten Cross Agency Priority (CAP) goals defined in the President's Management Agenda: Software Asset Management, Authorization Management, Mobile Device Management, Privileged Network Access Management, High Value Assets (HVA) System Access Management, and Data Protection. CDM will allow VA to meet the remaining three CAP goals.

Moving forward, VA continues to focus efforts on improving access control, governance, privacy and data protection, continuous monitoring, and configuration management processes and capabilities. VA also continues a shift from a reactive to proactive approach to its audit experience, reviewing previous audit findings to determine and enact appropriate remediation measures and improve audit scores in the future.

Department of Defense (DoD)/VA Collaboration

Seamless and secure interoperability is one of five imperatives under VA's modernization strategy. VA strives to streamline the Veteran experience by achieving seamless interoperability between VA and DoD, as well as other Federal and commercial partners. However, interoperability must also be secure; VA must augment

standardized and secure designs, interfaces, and processes to promote secure access to authoritative data.

To this end, VA is collaborating with DoD to jointly deploy standards and controls based on NIST and Committee of National Security Systems (CNSS) guidelines. VA's GRC tool and Enterprise Mission Assurance Support Service (eMASS) join VA and DoD under a shared RMF to facilitate joint cybersecurity activities. Finally VA, in coordination with DoD, is building a capable cybersecurity monitoring team. In the future, VA plans to explore paths to mutually designating jointly shared systems as National Security Systems (NSS). VA and DoD are working shoulder-to-shoulder to strengthen privacy and security for Veterans.

Workforce Management

In response to a shortage of cyber and privacy personnel across the Federal Government, VA has emphasized the development of a world-class technology workforce as one of its six focus areas. VA has implemented special programs and incentives to attract, recruit, and retain talented cyber and privacy professionals, cyber retention pay and benefits, and other internal and external training and reskilling opportunities. Most importantly, VA has found that candidates and employees are attracted to and continually inspired by the Department's mission. Employees understand the impact they have on Veterans. As a cyber-conscious organization, VA will continue to emphasize the immeasurable impact of cybersecurity on Veterans. By protecting Veteran data and VA information systems and ensuring secure services, cyber and privacy employees directly serve Veterans every day.

Quarterly Notice to Congress

On a quarterly basis, VA reports to Congress any breaches that occurred in the previous quarter, as mandated by Public Law 109-461 Veterans Benefits, Health Care, and Information Technology Act of 2006. For each data breach, the report identifies the Administration and facility responsible for processing or maintaining the sensitive personal information involved in the data breach and the status of any remedial or

corrective action. The report is signed by the Secretary and transmitted to the Chair and Ranking Member of both Senate and House Committees on Veterans' Affairs. This continuous reporting promotes transparency and cooperation between the Department and Congress. Within VA, reporting improves situational awareness and leads to an improved data security posture. For Veterans, this means that their personal information becomes even safer.

Conclusion

The complex issues before VA represent an opportunity for the Department to renew its commitment to protecting Veteran and employee data. The Department is modernizing its cybersecurity strategy to meet new Federal guidance and to keep pace with today's ever-evolving technology landscape. While expanding access for Veterans, VA is concurrently strengthening access control between the Department and its external partners. VA has established programs to constantly and consistently monitor cyber activity and identify gaps and new opportunities to mature its posture. VA is working shoulder-to-shoulder with DoD and our Federal and commercial partners to ensure seamless and secure interoperability that maintains the privacy and security of our Nation's heroes and VA's employees. Recruiting, developing, and maintaining a talented cyber and privacy workforce remains a priority and motivates human capital management efforts. VA continues to maintain compliance with Federally-mandated requirements such as Binding Operational Directives, Executive Orders, and Office of Management and Budget (OMB) memoranda. VA understands the challenge of maturing its cybersecurity posture while also improving access and services that Veterans want and deserve. With the above strategies, policies, and programs, the Department has risen to that challenge, and continues in its mission to protect and secure the information of, and services for, our Veterans. Madam Chair, Ranking Member, and Members of the Subcommittee, thank you for the opportunity to testify before the Subcommittee today to discuss one of VA's top priorities. I am happy to respond to any questions that you have.