STATEMENT OF KURT DELBENE
ASSISTANT SECRETARY FOR INFORMATION AND TECHNOLOGY
AND CHIEF INFORMATION OFFICER
OFFICE OF INFORMATION AND TECHNOLOGY (OIT)
DEPARTMENT OF VETERANS AFFAIRS (VA)
BEFORE THE
COMMITTEE ON VETERANS' AFFAIRS
SUBCOMMITTEE ON TECHNOLOGY MODERNIZATION
U.S. HOUSE OF REPRESENTATIVES

JUNE 7, 2022

Good afternoon, Chairman Mrvan, Ranking Member Rosendale, Chairman Takano, and distinguished Members of the Subcommittee. Thank you for the opportunity to testify today and discuss VA's cybersecurity program and initiatives to protect Veterans' data and VA information systems. I am accompanied today by Acting Chief Information Security Officer Lynette Sherrill. I want to begin by thanking Congress, and specifically this Subcommittee, for your continued interest and shared commitment to the success of VA's cybersecurity program. VA's mission to provide health services and benefits to Veterans and their support systems, while safeguarding their private information, is enriched by your unwavering support.

Since my arrival, we have redoubled our focus on cybersecurity. Despite this challenging time battling the COVID-19 pandemic, the Department has remained focused on carrying out its core mission of caring for those who borne the battle, and we remain vigilant in protecting Veteran and employee information and VA assets. The Department leverages sound cybersecurity practices to protect the confidentiality, integrity and availability of our information and information systems now and in the future. These practices include physical, technical and administrative controls designed to protect equipment, manage access and enable cybersecurity professionals to monitor, detect and respond to cyber threats. These protections constitute a strong defense in depth strategy comparable to those deployed in the commercial sector. This testimony will provide an overview of all VA currently does to protect Veterans' data, as well as note what challenges we currently face and where resources can best be allocated.

H.R. 7299, the Strengthening VA Cybersecurity Act

H.R. 7299 would require VA to conduct a third-party independent cybersecurity assessment. VA and Congress have the same goal when it comes to protecting Veterans' data. However, we believe the bill is unnecessary because VA already conducts a very broad and deep set of cybersecurity audits and evaluations using independent contractors that are equal to or beyond the requirements in the legislation.

Further, numerous reports and audits already being conducted address the concerns expressed in this bill. VA's Office of Inspector General (OIG) has two enterprise-wide annual audits that support the requirements in this bill: the Federal Information Security Modernization Act (FISMA) and the Federal Managers Financial Integrity Act (FMFIA). Under FISMA, VA uses an independent auditor to ensure the effectiveness of information security controls for federal systems that support our operations and assets. FMFIA requires Federal agencies, on an ongoing basis, to evaluate the adequacy of internal accounting and administrative systems, including processes to secure those systems. VA reports annually to the President and to Congress on the effectiveness of internal controls and any identified material weaknesses in those controls.

OIG assesses VA's information technology (IT) general and application controls. The independent audit conducted by OIG evaluates the effectiveness of security controls in security management, access management, contingency planning, configuration management and other National Institute of Standards and Technology-prescribed controls that would identify VA's capabilities against ransomware; denial-of-service attacks; insider threats; phishing; and threats to remote and telework capabilities. Additionally, OIG has added 20 IT security inspections across VA's data centers and facilities, which address the focus areas named in the legislation, including vulnerability management, evaluation of the use of IT systems and devices, information system component inventory, configuration management plan, baseline configuration, account management, session lock, identification and authentication (organizational users), audit events and logging, media sanitization, physical access controls, and other management; technical; operational; and privacy controls.

VA supports approximately 60 program or content specific audits each year under the direction of either OIG or the Comptroller General. More than 1,200 VA employees and contractors participate and support the audit process each year, with many more providing ancillary support. The independent, annual audits conducted in VA each year are provided on various system types and platforms, including high-value assets, cloud-based systems, facility-based systems, contractor-managed systems and systems that support mobile and remote capabilities. VA would be happy to brief the Committee on any areas of interest or the extensive audits that are in place, reviewing both findings and our progress in remediating any identified gaps or vulnerabilities. As written, the bill would provide us with the same findings as our current audits. The legislation would not do anything more substantive to strengthen our cybersecurity posture.

The VA's Approach Provides Rigor in VA Cybersecurity

VA deploys a diverse set of cybersecurity capabilities that protect the Department from threats. The cybersecurity capabilities include, but are not limited to, application layer firewalls; intrusion detection and prevention systems; web application firewalls;

email inspection and filtering; endpoint detection and response; traditional antivirus; web traffic decryption and inspection; enterprise predictive vulnerability scans; and forensic analysis. Collectively, these measures represent a strong defense-in-depth security strategy.

Security Excellence requires us to relentlessly evaluate and improve our cybersecurity program. The Department maintains system and information integrity through cybersecurity monitoring and reporting tools constantly searching for abnormal traffic patterns. VA also maintains strong partnerships with OMB, CISA, the Department of Health and Human Services, the Department of Homeland Security, the Federal Bureau of Investigation and the Department of Defense to leverage cybersecurity threat intelligence information containing indicators of compromise and adversarial tactics; techniques; and procedures.

Moreover, following Executive Order 14028 and the subsequent Federal Zero Trust Strategy (M-22-09) VA is leaning forward and anchoring the cybersecurity strategy with a Zero Trust First approach. VA already had made significant implementation of Multifactor Authentication across our applications and network, a critical component for safeguarding systems and users' identities in our Zero Trust Strategy. Security excellence integrates Zero Trust as part of OIT's larger realignment and weaves in my top priorities including People Excellence (cybersecurity hiring authorities), Engineering Excellence (not just fixing IT issues, but how can we do better next time) and Resource Allocation.

Addressing Cyber Vulnerabilities

As of May 17, 2022, VA does not have any open vulnerabilities rated as “critical” or “high” exposed publicly to the internet accessible systems[1]. VA has remediated 93% of CISA’s known-exploited vulnerabilities catalog and consistently maintains 90% or greater remediation of all critical and high vulnerabilities across the enterprise within our implementation timeline standard. VA achieved a 94.6% remediation of CVE-2021-4102 (Google Chrome Vulnerability); patched a critical vulnerability with a significant scope and scale within 14 days. CISA shared VA’s best practice with other Federal agencies who struggled to patch and scale critical vulnerabilities.

The Challenge of Recruitment and Retention

As stated previously, VA and Congress have the same goal when it comes to protecting Veterans’ data. While we continue to improve our cybersecurity posture, we do face recurring challenges, one of which is recruitment and retention of highly qualified personnel. Recruiting and retaining the most skilled individuals with high-demand cybersecurity expertise is a top priority for both OIT and industry leaders alike. For such employees, salaries are too low to be competitive, even when combined with compensation incentives and benefits. To successfully hire and retain high-demand

[1] Binding Operational Directive (BOD) 19-02.

cyber professionals, VA and the Federal Government must take immediate steps to increase the salaries of its GS-2210 workforce.

One possible solution is to implement a special salary rate. Through VA OIT's leadership of the Federal Cyber Workforce Management and Coordinating Working Group and in partnership with the Office of Personnel Management (OPM), we are currently leading an Interagency Project Team (IPT) to develop a government-wide Special Salary Rate (SSR) for GS-7 through GS-15 positions within the 2210-Information Technology Management occupational series. Leveraging labor market analysis conducted by the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Agency (CISA), IPT is working closely with OPM compensation experts and has the support of its leadership in developing SSR. The timeline for completion will be fiscal year (FY) 2023. Another partial solution could be to leverage Science and Technology positions for OIT personnel, although there aren't sufficient positions available to completely meet the need.

Conclusion

VA recognizes the challenges of maturing a cybersecurity posture while also improving access and services that Veterans want and deserve. With the strategies, policies and programs we have in place, the Department has risen to the challenge, and continues in its mission to protect and secure the information of, and services for, our Veterans. Mr. Chairman, 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.