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

November 20, 2024

Good morning, Chairman Rosendale, Ranking Member Cherfilus-McCormick, 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 Deputy Assistant Secretary for Information Security and Chief Information Security Officer Lynette Sherrill, and Deputy Chief Information Security Officer and Executive Director of Information Security Operations Jeff Spaeth. 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 my top priority as Chief Information Officer.

Since my arrival, the Department has remained focused on carrying out its core mission of caring for those who have 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 actions VA uses to protect Veterans' data, as well as note what challenges we face and where resources can best be allocated.

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 detection and prevention; 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 that constantly search for abnormal traffic patterns. Our CSOC analyzes all identified evidence of abnormal behaviors through automated and manual approaches to ensure that we take action on threats to the enterprise. VA also maintains strong partnerships with the Office of Management and Budget, the Cybersecurity and Infrastructure Security Agency, and 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 that provides indicators of compromise and information on adversarial tactics, techniques, and procedures.

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. For example, VA has achieved 97% enforcement 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 the Office of Information and Technology's (OIT) larger realignment and is integrated into our 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 part of VA's continued commitment to seeking independent assessments of our cybersecurity posture, we partner with the VA's Office of the Inspector General (OIG) to conduct enterprise-wide annual audits. VA respond to and act on recommendations from the OIG's Federal Information Security Modernization Act (FISMA) audit that included 25 recommendations for improving VA's information security program.

Beginning in 2020, the OIG also started an information security inspection program. Information security controls protect VA systems and data from unauthorized access, use, modification, or destruction. These inspections assess whether VA facilities are meeting federal and VA security requirements related to three control areas that the OIG determined to be at highest risk. Typically, facilities selected for these individual inspections were not included in the annual audit sample. OIG's inspections focus on configuration management controls, security management controls, and access controls. OIG has audited several VA facilities including VA's Dublin Healthcare System in Georgia, the Bedford VA Healthcare System in Massachusetts, VA's Financial Services Center in Austin, Texas, as well as the Enterprise Cloud Security and Privacy Controls.

Across these audits, OIT continually reviews the OIG's recommendations and implements remediations to help us combat the shifting and unprecedented threats a large health care system faces daily. For each audit, we respond to the OIG's findings by either 1) concurring and providing an action plan for resolution or 2) non-concurring and providing our grounds and evidence for that non-concurrence. In some cases, the OIG identifies a finding as a "repeat finding." In most cases, this is because that while the specific instances of the issue are different from year-to-year, the area of weakness remains when taken as a whole. For instance, cases of software patching untimeliness may be identified in multiple years. However, the actual instances identified from year-to-year will be different. The persistence of such issues as a category will cause the OIG to identify the area as one of continued weakness. Overall, we remain committed to acting on the most critical findings across all OIG's audit work, and it remains a valuable oversight tool for our organization.

The Challenge of Recruitment and Retention

Despite the efforts I just mentioned, we 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. We are concerned that salaries at VA may be too low to be competitive, even when combined with compensation incentives and benefits. Accordingly, in order to ensure that offers are competitive with those offered by industry, we support the Administration's legislative proposal in the "Civil Service Modernization Legislation for Cyber Workforce Positions" that would allow OPM to establish higher special rates—up to the rate for level II of the Executive Schedule—for cyber and certain other categories of employees on a Governmentwide basis.

A key part of VA's approach to make these positions competitive was the implementation of pay flexibilities in the PACT Act for GS-2210 employees. Our FY 2025 staffing and administrative support services request of $1.686 billion funds 8,310 FTE, which is 160 full-time equivalent employees (FTE) (2.0%) above the FY 2024 enacted level. An additional 139 FTEs are in the TEF request for FY 2025. As VA prioritizes key IT investments, we must also recruit, retain, and upskill our current IT workforce of over 8,000 FTEs. VA is working hard to modernize its workforce with targeted talent strategies, such as hiring for cybersecurity and artificial intelligence skills, continuous talent development, incentives, and focused field staff expansion to support Veteran health and benefits mission growth. The results of these efforts have been remarkable so far. OIT has experienced an 80 percent increase in highly technical applicants per job announcement since pay flexibilities were announced in Q2 FY23. Utilization of these pay flexibilities has contributed to 64 percent fewer separations and 46 percent fewer retirements, resulting in an estimated $13 million cost avoidance in the past calendar year.

The VA is also involved in Federal Government-wide workforce initiatives such the National Cyber Workforce Coordination group and Federal Cyber Workforce Working group to implement the National Cyber Workforce and Education Strategy as well as part of the working group to implement Executive Order 14119, "Scaling and Expanding the Use of Registered Apprenticeships in Industries and the Federal Government and Promoting Labor Management Forums." Further, VA announced a

Cybersecurity Apprenticeship Program for Veterans: a two-year developmental program within the VA Cybersecurity Operations Center (CSOC) to provide a unique, hands-on learning and development experience for cybersecurity apprentices and to encourage a career in the Federal cybersecurity workforce.

Executing the Strengthening VA Cybersecurity (SVAC) Act

President Biden signed the Strengthening VA Cybersecurity Act into law on December 27, 2022 (Pub. L. 117-302, or SVAC). Soon after, OIT entered into an agreement with MITRE to provide the Secretary with an independent cybersecurity assessment. MITRE's assessment reviewed five high-impact information systems as well as the effectiveness of the information security program and information security management of the Department.

MITRE's October 2024 report assessed Integrated Financial and Acquisition Management Systems (iFAMS), Loan Guaranty (LGY), Health Care Claims Processing System (HCPS), MyHealth*e*Vet (MHV, and VA Enterprise Cloud-Mobile Application Platform (VAEC-MAP). MITRE concluded that "[i]n fiscal year 2024, VA made significant strides in pursuing cybersecurity strategic goals with a risk-based approach to protecting Veteran data and ensuring the confidentiality, integrity, and availability of essential services for the Nations' Veterans." MITRE further stated that as a direct result of these efforts there has been a demonstrable improvement in VA's security posture.

As my July 2022 testimony to this committee stated would be the case, thanks to VA already conducting 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, the MITRE report did not identify a substantial number of "net-new" findings not previously known from VA's OIG two enterprise-wide annual audits: the FISMA and the Federal Managers Financial Integrity Act (FMFIA) audits. MITRE also found that the remediation actions detailed in its plan are covered within the scope of the Department's ongoing initiatives to reinforce and strengthen VA's cybersecurity risk posture. MITRE confirmed VA's existing audits are working as intended.

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.