STATEMENT OF
PAUL CUNNINGHAM, CHIEF INFORMATION SECURITY OFFICER
OFFICE OF INFORMATION SECURITY
OFFICE OF INFORMATION AND TECHNOLOGY
DEPARTMENT OF VETERANS AFFAIRS (VA)
BEFORE THE
SUBCOMMITTEE ON TECHNOLOGY MODERNIZATION
COMMITTEE ON VETERANS' AFFAIRS
U.S. HOUSE OF REPRESENTATIVES

MAY 20, 2021

Good morning Chairman Mrvan, Ranking Member Rosendale 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 Mr. Gary Stevens, Deputy Chief Information Security Officer, Executive Director for Information Security Policy and Strategy, Office of Information and Technology (OIT); Ms. Luwanda Jones, Deputy Chief Information Officer, Strategic Sourcing, OIT; and Ms. Martha Orr, Deputy Chief Information Officer, Quality, Performance and Risk, OIT. 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.

Introduction

Since I last briefed this Subcommittee 18 months ago, significant national and international events have altered how we operate and engage with Veterans. Despite this challenging time, 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.

From a cybersecurity perspective, the threats to our network remained the same throughout the pandemic. Our adversaries include nation-state actors, organized crime and individuals who have a nefarious agenda. Their motives continue to be financial gain, corporate or state-sponsored espionage, or damage to the Department's reputation and public trust. However, the COVID-19 pandemic fueled adversaries with new content that leveraged concern about the pandemic. For example, phishing campaigns were disguised as COVID-19 information updates, enticing users to "click on the link" they provided.

To respond to the pandemic, VA activated its fourth mission to improve the Nation’s preparedness for response to war, terrorism, national emergencies and natural disasters. Over the course of the past year, VA assisted state and local governments while continuing to provide services to Veterans during the national emergency. The Office of Information and Technology (OIT) worked aggressively to meet the demands of this new environment, identifying agile and flexible approaches to provide support to Veterans. Cybersecurity kept pace by revectoring efforts and providing agile, yet risk-based approaches to meet the demand of VA services.

VA’s Cybersecurity Program

Over the last year and half, the Department made significant progress in improving its overall cybersecurity posture, leveraging VA’s core cybersecurity objectives as a sturdy framework to address unprecedented challenges and opportunities. The increased emphasis on remote service offerings and reliance on remote work environments were areas where cybersecurity had a significant impact.

The Department was well-positioned to support COVID-19 response efforts, including the rapid expansion of telehealth because we made the investments in our technology early on and had a strong foundation in cybersecurity principles. OIT’s Office of Information and Security (OIS) expedited the security reviews of critical medical technologies, adjusted our risk threshold based on the operational constraints and provided security assessments for the enhancement of remote connections to VA’s networks. These actions enabled IT operations to continue uninterrupted delivery of health care, services and benefits to Veterans. OIT rapidly scaled and optimized VA’s network remote access so employees could continue working securely without unnecessarily risking exposure to COVID-19. As OIT increased network bandwidth and rapidly deployed cloud-based conferencing services, the cybersecurity team ensured Veteran data remained safe and secure.

VA’s cybersecurity response processes were tested in the past year, most notably during the SolarWinds event. Like many other departments and agencies, VA downloaded and installed the vendor-verified patch for SolarWinds that contained malicious software. This patch introduced malicious code into VA’s network. The Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency’s (CISA) issued Emergency Directive 21-01 to alert all Federal partners of the risk. VA complied with ED 21-01 and removed all instances of SolarWinds servers within 12 hours of notification. The Department engaged with CISA, Federal partners and commercial sources to obtain the indicators of compromise (IOC) specific to this threat. The team deployed all available IOCs to the cybersecurity monitoring toolsets, evaluated past network traffic and searched for other behaviors that would suggest successful exploitation of the vulnerability. No positive indicators were detected by VA or by our Federal partners. This event had no impact on VA’s mission critical activities, including its COVID-19 response and vaccination efforts, health care and telehealth infrastructure and VA’s Electronic Health Record Modernization (EHRM) program.

The Department continues to refine and improve its cybersecurity program with its core tenets as defined in the Federal Information Security Modernization Act (FISMA) and supported by the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Risk Management Framework. These foundational frameworks provide a cohesive, risk-based approach toward meeting mission objectives of the Department. VA's approach empowers cybersecurity personnel to engage with mission owners, business owners, system owners and technical staff to develop and deploy innovative technologies in a secure and effective manner. VA's cybersecurity program core objectives are:

1. Secure and protect VA and Veteran information;
2. Secure and protect VA's Information Technology (IT) infrastructure and systems;
3. Embed security in VA's future IT investments;
4. Enhance VA information security through external partnerships and information sharing; and
5. Drive down cybersecurity risk and resolve known weaknesses.

The Department must protect confidential data including Veteran and employee Personally Identifiable Information (PII) and Protected-Health Information (PHI). Data repositories, especially those that contain sensitive data, need to be appropriately secured and monitored. Likewise, information must be exchanged securely and across approved data transmission routes. Protecting data is critical in the expanding success of key programs such as telehealth and EHRM that are reliant on protected network and IT assets.

As VA continues implementing the EHRM program, the cybersecurity team identified additional partnership opportunities with the Department of Defense (DoD) to include aligning resources and common tools where appropriate. For example, the Department is leveraging the Enterprise Mission Assurance Support Service (eMASS) used by DoD to automate integrated cybersecurity management, reporting and continuous monitoring supporting Risk Management Framework processes. This capability bolsters VA's partnership with DoD and facilitates VA's and the Defense Health Agency's move to one Electronic Health Record system. VA also established a comprehensive cyber incident response process that is shared between DoD and VA.

Safeguarding VA Networks and Information Systems

Cyber threats are a real challenge as we see VA's networks bombarded daily. In any given month, we block over 130 million suspicious emails, block an additional 1.2 million spam emails and thwart over 6 million attempts to inject or install malware on our systems. The Department continuously maintains a vigilant posture, with defense-in-depth practices, sharing threat information with other Federal agencies, blocking suspicious IP addresses and emails, monitoring of endpoints and robustly searching for anomalous behavior. VA has established programs to monitor cyber activity, identify gaps and new opportunities to mature its posture.

The defense-in-depth approach includes reliance on VA's employees, Veterans and third-party vendors to protect our information and networks. The use of multi-factor authentication is an essential requirement to ensuring only authorized users are accessing VA’s networks and information systems. This, combined with system monitoring and regular system assessments, gives us confidence that individuals accessing our networks are authorized. We work on an ongoing basis with business owners to ensure that their applications are implementing cybersecurity best practices and applicable security requirements.

The Department shares the Administration’s vision of strength in partnerships and seeks to be an active and trusted partner in return. Through an open and trusted exchange of ideas, alerts and remediation strategies, the Department leverages the experience and perspectives of other cybersecurity programs providing a more stable and secure cybersecurity posture within. VA proactively shares cyber threat and information safeguarding information with our trusted partners, including the Federal Chief Information Officer Council, the Federal Chief Information Security Officer Council, Office of Management and Budget (OMB), National Security Council, Committee on National Security Systems, Information Sharing and Analysis Centers (ISACs) and third-party service providers.

Addressing Cybersecurity Challenges

VA is continuously seeking opportunities to enhance the protection of our information systems and drive down cybersecurity risk. The 2nd Quarter of Fiscal Year 2021 FISMA report was submitted on April 15, 2021, to OMB and DHS. In the Risk Management Assessment, VA was evaluated as “Managing Risk” overall, consistent with previous reporting periods. Additionally, VA met 7 of the 10 Cross Agency Priority goals defined in the previous administration’s President’s Management Agenda: Software Asset Management, Hardware Asset Management, Mobile Device Management, Privileged Network Access Management, High Value Assets System Access Management, Automated Access Management and Data Protection.

VA did not meet the target in three goal areas: Authorization Management, Intrusion Detection and Prevention, and Exfiltration and Enhanced Defense. For Authorization Management, VA reported 98 percent compliance against the OMB target of 100 percent. There are four high impact and three moderate systems operating without a current authorization. VA expects this to improve in the next 90 days. VA has improved in the Intrusion Detection and Prevention goal area from 97 percent to 99 percent in this part quarter. VA continues working toward the 100 percent target. The third goal not met is Exfiltration and Enhanced Defenses, which requires outbound traffic to be checked for unauthorized exfiltration. VA expects steady improvement as Data Loss Prevention capabilities are deployed throughout VA’s network. The Department has a long-term plan to cover our most sensitive networks by 2025.

The Department continues to take a risk managed approach to prioritize and improve cybersecurity efforts. The Office of Inspector General’s 2020 FISMA audit has highlighted areas of weakness in VA’s cybersecurity program. VA continues to make significant progress in implementing capabilities designed to improve its information security environment. VA has developed action plans for open findings and is taking a systematic approach to remediation, anticipating closure by 2025.

Supply chain risk management requires a VA-wide approach that incorporates multiple stakeholders including cybersecurity. Protecting our digital environment and ecosystems extends beyond our internal organizations to the products and services that are provided by third-party partners, vendors, suppliers, contractors, manufacturers, system integrators and consultants. VA is currently developing a strategy that identifies multiple stakeholders within the Department to reduce the risk posed by unsecure vendors. The Department must continue communicating operational, security and procurement requirements to suppliers ensuring that supply chain risks are appropriately addressed and mitigated.

Going forward, the Department is leveraging our proven success in risk management toward a more proactive and resilient IT infrastructure. We have several initiatives that support this perspective, beginning with the development of a new VA Cybersecurity Strategy that is forward thinking, while still balancing FISMA and NIST standards and guidelines and VA's mission requirements. The new Cybersecurity Strategy will be completed by September 2021. The Department is also examining changes in information processes and identifying innovative capabilities to improve the security of VA networks and information. These activities include exploration of new architectures; enhancing capabilities to protect data; and reducing the reliance on Veterans' social security numbers in information processing.

VA has embarked on an effort to improve visibility and monitoring of medical equipment. The first step is having an accurate inventory of medical equipment. VA has initiated testing and deployment of a specialized device asset management solution. When fully implemented, this solution will provide visibility of isolated specialized devices, including medical devices, special purpose systems and research scientific computing devices through device fingerprinting, alerting and displaying, asset discovery and recognition, vulnerability discovery and remediation management.

The Department is investing in people and technology to drive down cybersecurity risk and reduce vulnerabilities. The Office of Information Security has aligned the cybersecurity budget to the NIST Cybersecurity Framework to organize investments into basic cybersecurity activities, and VA continues to use direct hire authority to maintain a qualified professional cybersecurity workforce. We focus resources on information security investments toward a more resilient network and to better protect Veteran data and VA information systems.

Conclusion

The last year has proven that technology will continue growing as a mission enabler for the Department. Veterans have come to expect the same level of access and convenience in their engagement with VA as they experience with ubiquitous online activities. They also expect that their data are appropriately protected. VA's technical solutions must consider the interaction with users, the value to the Veteran, as well as the confidentiality, integrity and availability of VA's information resources. With a balanced, risk-managed approach toward secure computing, we will maintain the confidence and trust of Veterans, our stakeholders and the public.

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.