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 VETERANS' AFFAIRS
SUBCOMMITTEE ON TECHNOLOGY MODERNIZATION

FEBRUARY 12, 2020

Good morning Madam Chair Lee, Ranking Member Banks, and distinguished Members of the Subcommittee. Thank you for the opportunity to testify today about the Department of Veterans Affairs' (VA) mission to secure and protect the personal and sensitive information of our Nation's Veterans. I am Paul Cunningham, the Deputy Assistant Secretary for Information Security, Chief Information Security Officer (CISO) and Chief Privacy Officer. I am accompanied by Martha Orr, Deputy Chief Information Officer, Office of Quality, Performance, and Risk (QPR) within the Office of Information and Technology, and LaShaunne David, Director of VA Privacy Service within the Office of Information and Technology.

I want to thank Congress, and especially this Subcommittee, for its support of VA's work to ensure Veterans' privacy. Because of your steadfast cooperation, Veterans can continue to trust that their information is safe and secure. As the Chief Privacy Officer, I lead the VA's privacy program that protects Veterans' personal information. This aspect of VA's mission is personal to me. As a Veteran of the U.S. Navy, I fully share the concerns of my fellow Veterans who receive VA benefits, care, and services. For this reason, I am personally committed to ensuring Veterans' information is protected from exploitation and is handled with care.

Introduction

VA Secretary Robert Wilkie has pushed forward a Department-wide modernization strategy to transform the Veteran experience, including increased access to services and information and interoperability with the Department of Defense (DoD). To achieve this, VA must extend its digital footprint, introduce new technologies, and increase data sharing. However, such efforts bring new privacy and security considerations. VA understands that with IT modernization must come modernized privacy and security policies. VA's Assistant Secretary for Information and Technology and Chief Information Officer (CIO), Mr. James Gfrerer, and OIT are responsible for striking this balance among information technology (IT) modernization, IT operations, and privacy and security. Specifically, OIT's Office of Information Security (OIS) manages security and privacy policy and related activities Department-wide, while OIT's QPR division manages the VA Records Management program, which provides oversight of VA's compliance with those policies.

VA's mission is to provide Veterans the care, benefits, and exceptional service they have earned. In the course of that mission, Veterans voluntarily share their personal information with the Department. This information may include personally identifiable information (PII) such as an address or Social Security Number or protected health information (PHI) such as data captured during health care visits as well as PHI and PII information collected as part of their application benefits. Veterans may also provide information about their families or caregivers. An important part of VA's mission is to ensure we are good stewards of Veteran data.

VA has a robust set of policies and regulations governing privacy, access control, data and records management, and data sharing. It employs a rigorous framework of clauses and agreements that enforce these policies within VA and with our partners. VA also boasts strong incident response protocols to address any violation of these policies. In general, VA has policies and Business Associate Agreements that govern its activity or relationship with partners; conducts activities to enforce the policies; and imposes consequences for any violation of policy or contract agreement. With this strategy, VA effectively ensures the privacy of Veterans and the security of their personal information.

VA and many similar large organizations face challenges. As the Department moves to adopt and implement new technologies, its privacy and security policies and practices must keep pace and change accordingly. Emerging issues in technology require that VA continually emphasize the importance of privacy for our Veterans, the Department, and our Federal and commercial partners. As the Department rises to meet these challenges, VA remains a vigilant protector of Veterans' information.

Privacy Policy and Compliance

As part of VA's efforts to create a more seamless experience for Veterans, VA has increased ease of access to information on such sites as VA.gov. VA does not solicit personal information and only asks Veterans for information necessary to provide care or services. VA directly communicates to Veterans about the PII it collects and how that information will be used. The Department's policy regarding the privacy and security protection of Veteran data is accessible to Veterans on VA.gov and includes information about how VA collects, stores, uses, and discloses Veterans' information. It also details Veterans' legal rights and information about how VA complies with Federal regulations and user agreements. Like all Federal agencies, VA must comply with the Privacy Act, which provides protections for Veterans' personal information.

An example of proactive and tailored implementation of privacy policy is VA's Webpage privacy. VA maintains a general Webpage privacy policy, known as the "General Policy," that applies to all VA.gov Webpages. Some pages have additional guidance, called "Limited Privacy Policies," which are compatible with the General Policy. VA's Web sites generally do not require registration or request personal information, but some portals require Veterans to input PII to register for access. When Veterans do provide information, VA will not disclose that information to outside parties

except at the request of the Veteran or as authorized by law. Additionally, VA.gov will never sell or rent personal information to outside parties. Violation of any part of this policy within the Department would result in corrective actions including possible dismissal and could result in a criminal charge against the offending employee or contractor. These policies ensure that Veterans' digital experience remains as secure and confidential as a visit with their care provider.

VA also has a review process in place to ensure that Administrations and staff offices integrate privacy compliance into their development and use of IT systems. The VA Privacy Service implemented the Privacy Threshold Analysis (PTA), a tool to help identify potential privacy issues within each new IT system or project. In certain cases, VA staff may be required to complete a Privacy Impact Assessment, which helps Veterans understand what information VA is collecting and how the information will be used and stored. This process ensures that system owners and privacy officers work in tandem so that any new IT system or project addresses all privacy concerns for the Veteran. As VA modernizes old systems and develops new systems, this specific review process establishes a Department-wide consideration of privacy.

Access Control

VA has policies and practices to ensure that access to Veterans' information is strictly controlled. VA implements a role-based access control system, which means that the Department grants access only to those employees or contractors with an official need to know to perform essential job duties or health care functions. Often, VA must allow contractors or other third parties to access Veteran information in order to provide care or services; in these cases, the party enters into a clear, comprehensive, and strict agreement with VA about how it may or may not use that information. System owners under each of VA's Administrations must determine the level of access control to implement for the system containing VA data. Systems are not authorized to operate until a designated authorizing official reviews and determines the control configuration is acceptable. To maintain access to sensitive information, non-Department entities must protect VA data from access by any other outside party.

To enforce these policies and use agreements, system owners conduct regular audits for compliance with the Federal Information Security Management Act (FISMA) and routine checks to ensure the system is compliant. Additionally, audit logs contain information about who accesses the system, when the system was accessed, and what data were accessed.

Should data ever be improperly accessed, VA will act to restrict access to the system and initiate an incident review process to determine what happened. When the improper access was a result of human error or improper behavior, VA will take corrective actions which could range from remedial training to revocation of access. VA requires that all personnel including contractors undergo mandatory privacy and security awareness training and sign a National or Contractor Rules of Behavior agreement. The Department takes appropriate steps to enforce these agreements.

Data and Records Management

VA's Records Management policy governs the storage, transfer, and destruction of sensitive data within the Department. Sensitive information may only be stored on and transferred between approved systems or repositories or those which are governed by the appropriate access controls. Contractors and other third parties must also comply with VA requirements regarding media sanitization, and destruction must often be supervised by a Federal employee. From collection to destruction, Veterans' information is handled with the greatest possible care.

VA's QPR Enterprise Records Service oversees activities related to the creation, maintenance, and use of records and ensures compliance with National Archives and Records Administration VA Records Management policy and federal regulations that allow the release of limited Veteran information under the Release of Names and Addresses (RONA) program. When required by law, VA also provides information to the Veteran and the public in responding to requests submitted under the Freedom of Information Act (FOIA). Protecting Veteran data during this release is an extremely high priority. VA's OIS Privacy Service oversees activities related to safeguarding the PII and PHI of Veterans and employees. VA OIS Privacy Service's duties include:

- conducting privacy risk assessments and ongoing compliance monitoring of VA systems;
- overseeing information storage and VA's system of records;
- tracking access to PHI; and
- delivering privacy training, orientation, and ongoing awareness campaigns.

Should the VA OIS Privacy Service identify issues or receive complaints in the course of its oversight and monitoring, it will investigate and take corrective actions to enforce the Department's privacy policies in coordination with similar VA stakeholders and, when necessary, legal counsel.

QPR's Privacy and Records Assessment Division (PRAD) and its Administration partners perform onsite assessments on privacy and records management compliance at VA facilities and staff offices. Assessment findings that cannot be remediated onsite are reported to facility leadership for action. Issues that are not corrected as part of this ongoing continuous monitoring effort are further elevated to senior leadership as potential risk issues that could impact overall compliance. QPR's Risk Management Division will assign risk analysts to make determinations on the level of risk and determine overall required remediation actions.

Data Sharing and Portability

VA closely safeguards Veterans' information, but often must share data with partners to provide health care and exceptional service to Veterans. In general, VA does not share Veterans' information with non-Department entities, except when sharing is necessary to provide care or services to the Veteran or in accordance with routine uses as described in applicable system of records notices. In these cases, VA agrees with its partners about acceptable use of VA's systems and any Veteran information contained in those systems. That contract or agreement contains VA's requirements related to data protection and media sanitization, which the partner must meet to access Veterans' information. Once granted access to VA and/or Veteran information, it must protect that information as closely as VA does. These requirements are in place to ensure that Veterans' personal information is guarded just as closely, even when shared.

Conclusion

VA continues to improve the Veteran experience by consolidating health and benefits information in convenient digital platforms and increasing Veterans' access to their health records and data. However, VA understands that accessibility and sharing must not come at the expense of safety, security, and confidentiality. Additionally, emerging challenges in technology call for increased attention to data protection and privacy.

In response to these challenges, VA maintains a comprehensive security and privacy program. The Department strives to achieve the highest standards for safeguarding the sensitive information of our Nation's Veterans. We comply with Federal regulations, maintain an organizational structure focused on data protection and records management, and facilitate ongoing privacy assessments, reviews, and monitoring based on strict access controls.

Madam Chair, Ranking Member, and Members of the Subcommittee, thank you again for the opportunity to testify on behalf of the Department about the privacy safeguards we employ on behalf of the Veterans we serve and the exceptional service we strive to provide in the process.