

**STATEMENT OF  
MR. STEPHEN WARREN  
EXECUTIVE IN CHARGE  
OFFICE OF INFORMATION AND TECHNOLOGY  
DEPARTMENT OF VETERANS AFFAIRS  
BEFORE THE  
HOUSE COMMITTEE ON VETERANS' AFFAIRS  
NOVEMBER 18, 2014**

**Introduction**

Chairman Miller, Ranking Member Michaud, and Members of the Committee, thank you for the opportunity to appear before you today to discuss the Department of Veterans Affairs' (VA) Information Security.

**Scheduling**

Before discussing how VA's information security posture has improved over the past year, it is important to make a distinction between access to care and VA's information technology (IT) security efforts.

To my knowledge, there have been no indications that unauthorized individuals accessed the software; rather, some authorized users allegedly made inappropriate changes. Thus, there is no causal relationship between alleged internal data manipulation by certain VA employees and findings in VA's Office of Inspector General (OIG) Federal Information Security Management Act (FISMA) audit. As recently pointed out in OIG's recent report the limitations of the software underlying the scheduling system is secondary to the need for additional resources to actually schedule – doctors, nurses, and other health professionals; physical space; and appropriately trained administrative support personnel.

The limitations of the scheduling system and associated practices are being addressed. Resourcing recommendations for IT investments are made by each of the Administrations (Veterans Health Administration (VHA), Veterans Benefits

Administration, and the National Cemetery Administration) based on business priorities. VHA and the Office of Information and Technology (OIT) are working together to overhaul the outdated scheduling system and to bring an innovative scheduling program into VA's current electronic health record system - VistA. Empowering employees with the most useful and effective technology is key to transforming VHA. In the coming weeks, VA will release a Request For Proposal for acquiring new scheduling software, since the existing software was outdated and difficult to use. VA expects an interim milestone towards this acquisition in spring 2015. Through this process, VA held an Industry Day and engaged with VSOs for their input on what kind of a system would be best for Veterans.

The technology underlying the current scheduling system used by VA medical facilities is cumbersome and outdated. In addition, there is no audit capability in the scheduling application that will indicate whether users are manipulating data to meet wait time expectations versus making legitimate changes to appointment information. On May 12, 2014, as part of its investigation, the Office of the Inspector General (OIG) asked VA to enable audit controls on four Veterans Health Information Systems and Technology Architecture (VistA) files related to waiting lists. Once this request was received, VA immediately turned the auditing on for the requested items.

VA's current electronic health record, VistA, already has access and audit capabilities. VA is evolving its existing VistA system to meet or exceed all Federal information assurance requirements including the Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule, applicable National Institute of Standards and Technology special publications, and Federal Identity, Access and Credential Management policies.

## **Progress Made in Information Security**

VA employs an extensive, layered, defense-in-depth strategy to protect the security and confidentiality of VA information and information systems and we continue to make great strides to keep up with ever-evolving threats. We have established appropriate technical, physical, and administrative safeguards to help ensure the security and confidentiality of Veteran records. Since the June 4, 2013, hearing before the House Veterans Affairs Committee's subcommittee for Oversight and Investigations, we have acquired new monitoring capabilities, increased desktop security, and enhanced our speed in detecting and combating challenges.

Before we activate systems within our network, and before any Veteran's information is put into those systems, we take steps that ensure the information is protected to the best of our ability. The process for issuing formal approval to operate systems on VA's network – known as "Authorities to Operate (ATO)" – has greatly improved in the last year. We have migrated from a manual, point-in-time, paper process to an electronic, automated, continuous monitoring capability with the help of the newly implemented Governance, Risk, and Compliance (GRC) tool, which went live in August 2013. We are the first (and the largest) cabinet level government agency to have moved to continuous monitoring. This new capability allows VA to detect vulnerabilities early and respond to threats rapidly.

The GRC tool is not the only new addition to VA's security infrastructure. VA is working with our Federal partners, such as the Department of Homeland Security and VA is almost ready to implement the Office of Management and Budget's Trusted Internet Connection initiative.

As an organization of more than 300,000 employees, however, our biggest vulnerability is not technical. Physical exposure of VA data is the most significant risk facing our information security posture. Over 98 percent of the sensitive data exposure at VA is due to paper or human error-based incidents. Network and system safeguards are not technical absolutes – we must constantly remain vigilant in preventing human

error - such as an employee clicking a phishing link, mis-mailing a sensitive record, or losing an electronic device.

VA is addressing its ongoing challenge of protecting Veteran information on paper by focusing on our employees. Because VA employees are the first line of defense when it comes to information protection, VA is working to improve employee awareness of information protection through training and other measures. VA promotes an environment where all employee's and contractor's actions reflect the importance of information security accountability.

In addition, every VA employee, contractor, and volunteer is required to sign a "Rules of Behavior" statement that sets expectations and makes clear that users are accountable for the protection of sensitive information. Every employee, contractor, and volunteer is also required to take an annual Information Security and Privacy Training. System access is terminated if individuals are delinquent. If a security or privacy incident occurs involving an employee or group of employees, VA employs recovery activities that include re-training of those involved. In addition, VA runs an annual Information Security and Privacy Awareness Week and sends out monthly messages reminding employees about security and privacy best practices. Educating our workforce is an ongoing process that VA takes very seriously.

The Department has established a rigorous data breach notification process. Once a reported incident is evaluated by the Incident Resolution Team, it is forwarded to the Data Breach Core Team (DBCT). The DBCT performs a risk analysis on all reported data breach incidents and when they determine a potential breach may have occurred and may pose a reasonable risk of harm to the affected individuals, they recommend that those individuals be notified and, if appropriate, offered free enrollment in a credit monitoring service to mitigate any risk of identity theft or improper use of their information. This robust review process is complemented by the monthly posting on VA's Web site of notifications of any data breaches, and this material is also provided to Congress through VA's quarterly data breach reports.

## **FISMA**

FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. OIG conducts annual FISMA audits of the agency's information security program. VA appreciates OIG's time and effort conducting its annual FISMA report, and appreciates that OIG finds VA's comments and corrective action plans as responsive to its recommendations. Although much work remains, VA has made significant improvements in the last few years and strives to meet the highest standards in protecting sensitive information. We are constantly and continuously improving our information security posture so that we may be the best possible stewards of Veteran information.

## **Federal Information System Controls Audit Manual (FISCAM)**

The Government Accountability Office FISCAM is designated to be used during financial and performance audits and may result in the identification of material weaknesses. The most recent FISCAM audit review reflects that we have closed out many of the observations from prior years, and are making considerable improvements each year. In a constantly changing threat landscape, we continue to evolve.

The number of FISCAM findings has decreased 29 percent since fiscal year 2011. Highlights of VA's accomplishments in this area include:

- VA has resolved its findings on contingency planning, as well as segregation of duties.
- VA reduced the amount of time needed to complete a scan of the entire enterprise from approximately 1 year to approximately 1 month.
- VA completed two-factor authentication for system administrators.
- VA strengthened passwords critical to accessing systems.

OIG noted our compliance in the above areas, and now looks to us to maintain consistency across the enterprise. VA leadership remains engaged in order to remediate the recommendations made by OIG.

## **Conclusion**

Over the past year, VA has made demonstrable progress improving upon its defense-in-depth strategy to protect Veteran information and VA systems. VA has made progress in FISMA audits, in the tools we use to combat evolving cybersecurity threats, and in securing the systems our clinicians and employees use to serve Veterans. We continue to work to address the challenges we face, including continued work to close FISMA recommendations and better educating employees on handling sensitive information on paper. We will continue to ensure our IT systems, which are crucial to supporting our Veterans, are secure and our employees are responsible as we protect the information of the Veterans we serve.