**STATEMENT OF**

**STEPHEN W. WARREN**

**ACTING ASSISTANT SECRETARY FOR INFORMATION AND TECHNOLOGY,**

**DEPARTMENT OF VETERANS AFFAIRS,**

**BEFORE THE**

**SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATION,**

**HOUSE COMMITTEE ON VETERANS’ AFFAIRS**

**June 4, 2013**

**Introduction**

Chairman Coffman, Ranking Member Kirkpatrick, members of the Subcommittee: thank you for inviting me to testify regarding the Department of Veterans Affairs’ (VA) Information Technology (IT) security strategy. I appreciate the opportunity to discuss VA’s plans, actions, and accomplishments in IT security.

Protecting the data that VA holds on Veterans is as important as the Veterans themselves. As the committee knows, the Department received a wakeup call from the incident in 2006 involving a stolen laptop which contained unencrypted information on over 19 million Veterans. As a result of this incident, VA consolidated its disparate IT functions into a single, unified IT organization. This consolidation has benefited VA in many ways, especially in terms of strengthening its information security posture. VA’s consolidated IT organization is responsible for protecting Veteran information at 153 hospitals, 853 community-based outpatient clinics, 57 benefits processing offices, and 131 cemeteries and 33 soldier’s lots and monument sites. Our network supports over 400,000 users, and over 750,000 devices.

We remain committed to protecting the information we hold on millions of Veterans and their beneficiaries and more than 300,000 VA employees by providing round-the-clock security of VA’s enterprise and infrastructure. The Department fully supports the White House’s information security initiatives such as two-factor authentication using HSPD-12 compliant PIV cards, which the VA is in the process of implementing. The Department continues to improve the security posture of the VA network through our Visibility into Everything initiative, which allows VA to see and manage all of its devices and network components in real time. The continuous monitoring program is responsible for checking IT systems and monitoring every desktop and laptop computer attached to the VA network.

To reinforce our commitment to information security, we are fostering a culture change to ensure that all users on our system follow all necessary and required IT and privacy protection rules. VA launched the Continuous Readiness in Information Security Program (CRISP) in 2012 to proactively address process and policy deficiencies and architecture and configuration issues. As part of the CRISP effort, VA conducts rigorous vulnerability scanning, continuous monitoring of patching and software inventory, implementing port security, anti-virus services, and encryption of non-medical IT laptops.

Through Web Application Security Assessments, VA is able to identify critical vulnerabilities and potential exploits in VA applications that store millions of records of sensitive data. The network infrastructure is protected through identification of all network assets and critical database stores, identification of all connections, and providing the Trusted Internet Connection Gateways services for mail, content filtering, name resolution and firewall protection.

In the past year, VA improved its security posture. The Department has ensured that over 98 percent of VA staff have received the mandatory information security training they need to protect the information of Veterans and their families. We have also completed a number of business impact assessments for contingency planning.

After the 2006 laptop incident, VA worked to ensure its laptop computers were encrypted to provide another layer of protection. Currently, over 98 percent of VA’s non-medical IT laptops are encrypted. VA has around 2,500 unencrypted laptops remaining and, with the exception of laptops with specific waivers (specific medical uses, research laptops using software where encryption would disable the device, service/maintenance laptops that do not connect to VA’s network or store sensitive information, and laptops purchased by VA and given to Veterans as part of a A rehabilitation program) the Department expects to complete encryption of all laptops by June 30, 2013.

**Data Breaches**

The Department has worked hard to regain the trust of Veterans after the stolen laptop incident in 2006. VA now has a robust data breach notification process, using a Data Breach Core Team (DBCT), which provides advance planning, guidance, analysis, and direction regarding the potential loss of Protected Health Information (PHI), Personally Identifiable Information (PII), or both. The DBCT serves as the decision making body between the functional area(s) affected, VA organizations, and external stakeholders.

The DBCT is made up of representatives from across nearly every part of the VA enterprise. When the DBCT determines that a breach is reportable, notification is made to the affected individuals and credit monitoring is extended. VA also posts a monthly report of data breach notifications on its Web site and holds a press call with reporters to discuss the contents of the report. The report is also provided to Congress, in addition to a quarterly data breach report.

VA has become one of the very best large organizations at providing notification when a breach occurs. For example, while the HITECH Breach Notification Rule requires covered entities to provide notification within 60 calendar days after discovery of the breach, and the strictest state laws require notice within 45 days after discovery of a breach, VA policy requires notification within 30 days. A review of VA’s incident tracking system over the current fiscal year indicates that VA takes, on average, 25 days to provide notice.  VA’s standards and practices exceed even the strictest Federal and state laws and policies.

**Conclusion**

Mr. Chairman, VA places the highest priority in safeguarding Veterans’ and employees’ personal information. We are committed to information security, and although work remains, VA has made significant improvements made in the last few years and strives to meet the highest standards in protecting sensitive information. Thank you for your continued support of Veterans, their families, and of our efforts to protect Veterans and their private information. I am prepared to answer any questions you and other Members of the Subcommittee may have.