STATEMENT OF
MAUREEN REGAN
COUNSELOR TO THE INSPECTOR GENERAL
OFFICE OF INSPECTOR GENERAL
DEPARTMENT OF VETERANS AFFAIRS
BEFORE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
COMMITTEE ON VETERANS' AFFAIRS
UNITED STATES HOUSE OF REPRESENTATIVES
HEARING ON INFORMATION SECURITY MANAGEMENT AT THE DEPARTMENT OF VETERANS AFFAIRS – CURRENT EFFECTIVENESS AND NEED FOR CULTURAL CHANGE

February 28, 2007

INTRODUCTION

Mr. Chairman and Members of the Subcommittee, I am pleased to be here today to address the Office of Inspector General's (OIG's) oversight efforts of the Department of Veterans Affairs (VA) Information Security Program, its effectiveness, and the need for cultural change in VA to further improve and strengthen information security. Today, I will present our observations and identify the information security challenges VA must continue to address in order to ensure information security in VA. With me today is the Deputy Assistant Inspector General for Auditing, who will help answer questions about our audit work related to information security.

To improve the Department's information security posture, VA's senior management needs to effectively secure the Department's information assets. This includes the entire set of information technology (IT) systems and technological infrastructure, as well as all sensitive information and data under VA's control. It is critical that effective controls and monitoring mechanisms be in place to ensure compliance with applicable Federal standards and all VA policy requirements. Protecting VA information and data is, and must remain, a primary focus of the Department. Our observations indicate that VA needs a culture change throughout the Department to gain reasonable assurance of VA-wide compliance with Federal and Department information security regulations, policies, procedures, and guidance.

OIG HAS REPORTED CONTINUING WEAKNESSES IN INFORMATION SECURITY

Our audits and evaluations on information security and IT systems have shown the need for continued improvements in addressing security weaknesses and support the need to change VA's culture. We reported VA information security controls as a material weakness in our annual Consolidated Financial Statements (CFS) audits since the fiscal year (FY) 1997 audit. Our annual Federal Information Security Management Act (FISMA) audits have identified continuing information security vulnerabilities every year since FY 2001. We have also reported IT security as a major management challenge for the Department from FY 2000 to the present. As a result of these vulnerabilities, we recommended that VA pursue a more centralized

approach, apply appropriate resources, and establish a clear chain of command and accountability structure to implement and enforce internal controls.

During the period 2000-2005, we reported that persistent repeat findings and weaknesses existed for physical, personnel, and electronic security and concluded that VA had not taken sufficient actions to correct the information weaknesses in our previous FISMA reports. Also, our work has continued to identify that corrective actions are not implemented at all VA facilities.

We observed that management of data centers and several program offices have taken actions to remediate elements of information security control weaknesses reported in our prior reports. However, VA's program and financial data continue to be at risk due to significant weaknesses related to the lack of effective implementation and enforcement of agency-wide security controls. These weaknesses place sensitive information, including financial data and veterans' medical and benefit information, at risk of unauthorized access, improper disclosure, alteration, theft, or destruction, possibly occurring without detection.

Prior to the May 2006 data loss, VA's information security program showed significant security vulnerabilities. VA's CIO reported he did not have sole authority to implement all aspects of the VA-wide IT security program within VA's Administrations. IT infrastructure was decentralized because VA believed that decentralized operations provided better management of VA facilities. Finally, VA lacked adequate agency-wide security control policies and procedures to provide effective guidance and organization standards.

VA has not fully implemented any of the recommendations on information security from our previous FISMA reports. In our ongoing 2006 FISMA audit, we determined that all 17 recommendations cited in prior FISMA reports remained unimplemented. In addition, we anticipate identifying several new high-risk areas associated with certification and accreditation of VA systems, remote access, and access to sensitive information by non-VA employees. Until all matters are fully addressed by the Department, VA systems and VA data remain at risk.

In some areas, however, the Department has made progress. Since the May 2006 data breach, VA has initiated positive steps focused on policies, awareness, and training. For example, all VA employees were mandated to complete information security awareness training. In addition, in 2006, VA took initial steps toward implementing a more centralized Department-wide IT security program under the direction of the Department's CIO. However, establishing and implementing an effective centralized Department-wide IT security program will require more time and effort.

VA DOES NOT ADEQUATELY PROTECT SENSITIVE INFORMATION FROM DISCLOSURE

The May 2006 theft of an employee's personal hard drive containing personal information on at least 26.8 million veterans, active military, and dependents, has been characterized as the largest data breach ever in the Government. The employee, who was authorized access to the data, copied large amounts of protected information onto portable devices and took it home without authorization. The data was not encrypted or password-protected.

The incident was a wake-up call for VA because it identified the lack of effective policy and internal controls to protect sensitive information from theft, loss, or misuse by VA and contract employees. Our review found a patchwork of policies that were difficult to locate and fragmented. None of the policies prohibited the removal of protected information from the worksite or storing protected information on a personally-owned computer, and did not provide safeguards for electronic data stored on portable media, such as laptop computers.

The potential loss of protected information not stored on a VA automated system highlighted a gap between VA policies implementing information laws and those implementing information security laws. We found that policies implementing information laws focused on identifying what information is to be protected and the conditions for disclosure; whereas, policies implementing information security laws focused on protecting VA automated systems from unauthorized intrusions and viruses. As a result, VA did not have policies in place at the time of the incident to safeguard protected information not stored on a VA automated system.

We found that policies implemented by the Secretary since the incident were a positive step in the right direction; however, we determined that more needed to be done to ensure protected information is adequately safeguarded. We determined that VA needed to enhance its policies for identifying and reporting incidents involving information violations and information security violations to ensure that incidents are promptly and thoroughly investigated; the magnitude of the potential loss is properly evaluated; and that VA management, appropriate law enforcement entities, and individuals and entities potentially affected by the incident are notified in a timely manner.

To address these deficiencies, we recommended that the Secretary take the following actions in our report, *Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans* (Report Number 06-02238-63, July 11, 2006).

- Establish one clear, concise VA policy on safeguarding protected information when stored or not stored in VA automated systems, ensure that the policy is readily accessible to employees, and that employees are held accountable for non-compliance.
- Modify the mandatory Cyber Security and Privacy Awareness training to identify and provide a link to all applicable laws and VA policy.
- Ensure that all position descriptions are evaluated and have proper sensitivity level designations, that there is consistency nationwide for positions that are similar in nature or have similar access to VA protected information and automated systems, and that all required background checks are completed in a timely manner.
- Establish VA-wide policy for contracts for services that requires access to protected information and/or VA automated systems, that ensures contractor personnel are held to the same standards as VA employees, and that information accessed, stored, or processed on non-VA automated systems is safeguarded.

- Establish VA policy and procedures that provide clear, consistent criteria for reporting, investigating, and tracking incidents of loss, theft, or potential disclosure of protected information or unauthorized access to automated systems, including specific timeframes and responsibilities for reporting within the VA chain-of-command and, where appropriate, to OIG and other law enforcement entities, as well as appropriate notification to individuals whose protected information may be compromised.

The Secretary concurred with the findings and recommendations in our report and agreed to implement the recommendations. On February 9, 2007, the Assistant Secretary for Information and Technology and his staff provided us with a briefing on the status of the recommendations in the report. Although an implementation process was discussed using an electronic database with a matrix that showed what issues needed to be addressed, we were not provided an implementation plan or any supporting documentation, such as draft policies, to show progress made in implementing the recommendations. To date, all 5 recommendations remain open, although VA has developed a new Privacy Awareness training module. It was circulated to all VA Privacy Officers, including the OIG's Privacy Officer, for review and comment. We reviewed the module and confirmed that it provides a link to applicable laws and VA policy. When implemented, the module will meet the intent of one of our recommendations.

Shortly after the May 2006 incident, VA issued policies to address information security. On June 7, 2006, the Secretary issued VA Directive 6504, *Restrictions on Transmission, Transportation and Use of, and Access to, VA Data Outside VA Facilities*, and it is available to all employees on VA's directives website. VA Directive 6504 contains policy for 23 different items. As stated in our report, we found that the Directive was difficult to understand; too technical for the average employee to understand; used terms, such as "appropriate" that were too vague to ensure compliance; and made reference to other applicable, policies, guidelines, and laws without identifying them.

Notwithstanding these concerns, we considered VA Directive 6504 to be a step in the right direction. The Directive prohibits the use of non-VA owned equipment to access the VA Intranet remotely or to process VA protected information except as provided in the Directive. In addition to requiring the use of encryption software on computers used outside VA facilities, a key provision in the Directive is that only VA-owned equipment, including laptops and handheld computers, may be used when accessing VA systems remotely. However, these requirements have not been implemented throughout VA. On October 5, 2006, VA issued a Memorandum, IT Directive 06-5, approving a temporary waiver for all three VA Administrations. Although the VA personnel were required to use approved encryption software when using non-VA hardware, VA does not provide the software. In addition, neither VA Directive 6504 nor IT Directive 06-5 contain provisions stating how VA will ensure compliance.

There is a greater awareness in VA regarding the issue. However, VA still lacks effective internal controls and accountability which leaves sensitive information at risk.

VA CONTINUES TO REPORT ONGOING DATA INCIDENTS

VA's Security Operations Center (SOC) is responsible for managing, protecting, and monitoring the cyber security posture of the agency. In July 2006, VA began sending us information on incidents from the SOC, providing information on a variety of incidents such as unauthorized access; missing, stolen, or lost laptop computers; improper disposal; and numerous incidents involving unencrypted e-mail messages containing sensitive information.

To date, these reports have covered about 3,600 incidents and the SOC has referred over 250 incidents to us, which resulted in us opening 46 cases to investigate. SOC reports do not always include indications of the magnitude of the data breach, that is, the number of individuals with personally identifiable information related to the incident. We have no way to determine the number and magnitude of incidents that occurred and were not reported to the SOC, nor can we verify the accuracy on the reported number of individuals affected by data incidents listed in SOC reports.

Since the May 2006 incident, the OIG has remained committed to investigating significant data loss cases that show that VA or contract employees are not taking the steps necessary to protect sensitive information. For example, the incident involving the theft of a computer owned and maintained by Unisys, containing sensitive VA information, shows that information provided to contractors' is also at risk. In our ongoing investigation of the data loss at Birmingham, Alabama, we continue to find that VA sensitive information was not protected.

CONTINUING CHALLENGES

Information security weaknesses persist at VA despite the findings and recommendations made in our reports. Most VA data remains unencrypted, including data transmitted by electronic mail over the internet. Although the Department has begun action, it still does not know how many VA employees and contractors use non-VA computers to remotely access VA systems. In addition, VA has not determined how many external hard drives or other portable devices are in use throughout VA. Finally, VA does not know what VA data is stored on these computers, external hard drives, or other portable devices. VA also has no means to monitor whether access to data by employees and contractors is limited to the information needed to conduct business**.**

Policies and procedures issued to safeguard protected information will not be effective unless there is compliance by all employees and contract personnel who have access to the information. Local management needs to conduct adequate oversight to ensure compliance and hold employees and contractors accountable for non-compliance. VA must ensure that managers and supervisors are held accountable for implementing the policies and procedures. In addition, VA must invest in the resources needed to provide employees with the hardware and software needed to conduct business and, at the same time, protect sensitive information.

Implementing the controls needed to ensure that sensitive information is protected will require that VA employees change the manner in which they currently conduct business. VA must find a way to implement these controls without impacting VA's ability to meet its mission.

In closing, I would like the Subcommittee to know that oversight and reviews of the effectiveness of VA's information security will remain a priority for the OIG until these issues are addressed. We remain committed to assessing the adequacy of information security controls and we will remain dedicated to protecting our Nation's veterans along with their personal and sensitive information. Mr. Chairman and Members of the Subcommittee, thank you again for this opportunity to update you on the status of our ongoing work. We are happy to answer any questions.