STATEMENT OF
BELINDA J. FINN
ASSISTANT INSPECTOR GENERAL FOR AUDITS AND EVALUATIONS
OFFICE OF INSPECTOR GENERAL
U.S. DEPARTMENT OF VETERANS AFFAIRS
BEFORE THE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
COMMITTEE ON VETERANS' AFFAIRS
UNITED STATES HOUSE OF REPRESENTATIVES
HEARING ON
"ASSESSING INFORMATION SECURITY AT THE
U.S. DEPARTMENT OF VETERANS AFFAIRS"
MAY 19, 2010

INTRODUCTION

Mr. Chairman and Members of the Subcommittee, thank you for the opportunity to discuss the Office of Inspector General (OIG) work on VA's implementation of the *Federal Information Security Management Act of 2002* (FISMA), which requires that VA develop, document, and implement an agency-wide information security program. Accompanying me is Mr. Michael Bowman, Director, Information Technology and Security Audits. In March 2010, we issued a report, *Fiscal Year 2009 - Federal Information Security Management Act Assessment*, that provided 40 recommendations for improving VA's information security program.

Seven years after FISMA's enactment, we continue to report significant deficiencies with controls supporting VA's information security program, which could have potentially alarming consequences. While VA has made progress defining policies and procedures supporting its agency-wide information security program, it faces significant challenges implementing effective access controls, system interconnection controls, configuration management controls, and contingency planning practices designed to protect mission critical systems from unauthorized access, alteration, or destruction. Because of the significant security deficiencies, the OIG's independent financial statement auditors concluded that VA's implementation of its agency-wide information security program constitutes a material weakness for financial reporting. I will focus on VA's progress and the challenges it faces in implementing key elements of its information security program and system security controls.

BACKGROUND

Sound information security practices are vital to the Federal government because secure systems and networks are needed to support critical programs and operations. The need for a vigilant approach to information security is apparent as demonstrated by well publicized reports of information security incidents, the wide availability of hacking tools on the internet, and the advances in the effectiveness of attack technology. Without proper safeguards, VA computer systems are vulnerable to intrusions by groups with malicious intent, who can obtain sensitive information, commit fraud, disrupt

operations, or launch attacks against other systems. In the past, VA has reported security incidents in which sensitive information has been lost or stolen, including personally identifiable information, exposing millions of Americans to the loss of privacy, identity theft, and other financial crimes.

Concerned by reports of significant weaknesses in Federal computer systems, Congress passed FISMA in 2002, which requires agencies to develop and implement an information security program, evaluate security processes, and provide annual reports. FISMA sets forth a framework for establishing information security controls over systems that support Federal operations and requires annual independent evaluations by the Inspectors General or independent external auditors. To assess compliance with the requirements of FISMA, the Office of Management and Budget (OMB) prepares annual reporting instructions requiring each agency to provide information summarizing their ability to secure their information systems and data. Additionally, OMB requires the Inspectors General to independently evaluate the agency's performance in a number of security areas and provide their results to OMB as part of the annual reporting requirements under FISMA. Historically, OMB's annual reporting instructions have focused on whether agencies have developed appropriate policies, procedures, and practices supporting their information security program. While our work has addressed OMB's reporting requirements, we have also performed comprehensive testing of general and technical information security controls that are designed to protect VA's mission critical systems and data. We believe our audit findings and recommendations provide a solid foundation for improving the effectiveness of VA's information security program and assisting VA in meeting the information security objectives of FISMA.

OIG AUDIT RESULTS

Our annual audit work includes determining the extent VA complies with FISMA's information security requirements, information security standards developed by the National Institute of Standards and Technology, and the annual reporting requirements from OMB. During our work, we assess VA's information security policies and procedures, observe operational controls, and test technical controls over general support systems and major applications.

Information Security

Our fiscal year (FY) 2009 review found VA made progress implementing elements of its agency-wide information security program. In recent years, VA issued VA Directive and Handbook 6500, *Information Security Program*, to define high level policies and procedures supporting its agency-wide information security program. In FY 2009, VA initiated the formal certification and accreditation of approximately one-third of its major systems—a process designed to provide assurance that security controls are adequately protecting critical systems and data. Also, VA conducted privacy impact assessments on many systems with the goal of identifying and reducing unnecessary holdings of personally identifiable information throughout all VA systems. VA has also established a new risk assessment methodology that addresses deficiencies identified by the OIG in prior years. Recently, VA implemented some technological solutions,

such as secure remote access, application filtering, and portable storage device encryption to improve the security control protections over its mission critical systems and data.

In addition to our audit work, VA's Certification and Accreditation Program and internal security reviews have identified over 11,000 plans of action and milestones (action plans) that need to be addressed to remediate system security deficiencies. In the near term, VA must complete a large number of these action plans to provide assurance that system security controls adequately protect mission critical systems. Our testing identified a significant number of action plans that were prematurely closed without sufficient documentation or testing to demonstrate that system security weaknesses were fully addressed. Without adequate testing and supporting documentation, VA cannot justify the closure of the action plans or provide assurances that corresponding information security risks were fully mitigated or eliminated.

Access Controls

During system testing, we identified significant weaknesses with access controls designed to protect VA mission critical systems from unauthorized access, alteration, and destruction. For example, we identified a large number of weak passwords on application servers, databases, and networking devices supporting systems at most VA facilities tested. The presence of weak passwords is a well-known security vulnerability that allows malicious users to easily gain unauthorized access to mission critical systems.

We noted that password settings were not configured to enforce strong passwords on some financial management systems and domain controllers. As identification and authentication controls are primary defense mechanisms against password attacks, enforcement of a strong password policy is essential for preventing unauthorized access to these systems. We also identified numerous user accounts with unnecessary system privileges and unauthorized user accounts that were not supported with formal access authorizations. To enforce comprehensive access controls, VA needs to periodically review system user accounts to ensure that system permissions do not exceed the users' functional responsibilities.

Network access controls are important for providing logical security over interconnected systems and data. We noted that most VA medical facilities were not appropriately using network segmentation to restrict access to their sensitive medical devices and network segments. Consequently, we were able to gain unauthorized access to sensitive sub-networks while at VA medical facilities and from remote locations throughout the enterprise. The proper use of network segmentation for restricting access to sensitive medical devices is critical for the security and operational stability at VA's medical centers.

System Interconnections

During testing of system interconnections, we noted that VA had not identified, managed, or monitored a significant number of VA system connections. In many cases,

VA had not maintained appropriate interconnection agreements to establish and govern the security requirements for those external network connections. VA is in the process of cataloging all system interconnections, but unknown system interconnections may exist. The lack of comprehensive monitoring of the external network interconnections prevents VA from effectively detecting and responding to network intrusion attempts in accordance with FISMA. Consequently, an attacker could penetrate VA's internal network and systems over an extended period of time without being detected. To improve its ability to monitor and respond to malicious network activity, VA plans to reduce and consolidate all external network connections into four major gateways over the next several years.

Configuration Management

Configuration management controls ensure that only authorized, tested, and protected systems are placed into operation. We identified significant weaknesses with configuration management controls designed to protect VA's mission critical systems and data from unauthorized access, alteration, or destruction. More specifically, our testing revealed unsecure web application servers, critical application servers hosting vulnerable third-party applications and system software, and user permissions that exceed the user's functional responsibilities on critical database platforms.

For example, we identified several instances of VA hosting unsecure web services that could allow a malicious user to exploit certain vulnerabilities and gain unauthorized access to VA systems. Our testing identified several VA websites using outdated encryption modules and one website accepting sensitive information over unencrypted internet sessions. We also noted several database platforms providing system functions or hosting outdated system software that could allow any system user to gain unauthorized access to mission critical data and potentially alter the operation of the database. To improve performance in this area, VA needs to implement a comprehensive enterprise-wide patch and vulnerability management program that will continuously identify and remediate security vulnerabilities impacting mission critical systems.

Contingency Plans and Testing

Our review of system contingency plans and testing revealed many instances where VA facilities did not validate whether system owners could restore mission critical systems at a remote processing site to ensure continuity of operations. In its annual FISMA report to OMB, VA reported it had successfully tested the viability of 93 percent of its system contingency plans. Based on our sample, VA provided evidence that only 56 percent of its system contingency plans were successfully tested. Our information was derived from evaluating evidence of actual system contingency plan test results while VA compiled information reported from local managers.

During testing, some VA facilities performed "table-top" testing which involved high level discussions of recovery procedures. However, "table-top" testing does not involve deploying equipment and personnel, and should not be considered a substitute for full contingency plan testing. Without in-depth and realistic contingency plan testing, VA

cannot provide assurance that mission critical systems can be readily restored in the event of a disaster or a service disruption.

Recommendations and Corrective Actions

Our FY 2009 report provided 27 current recommendations to the Assistant Secretary for Information and Technology for improving VA's information security program. The report also highlighted 13 unresolved recommendations from prior years' assessments for a total of 40 outstanding recommendations. During FY 2009, VA successfully addressed eight outstanding recommendations from our prior FISMA assessments.

Overall, we recommended that VA focus its efforts in the following areas:

- Remediating information security weaknesses that contribute to the material weakness reported in the annual audit of VA's consolidated financial statements.
- Taking an agency-wide approach for addressing action plans as opposed to developing corrective actions based on specific sites and systems.
- Establishing effective processes for identifying and responding to malicious network activity.
- Implementing automated mechanisms for the continuous monitoring and remediation of security weaknesses impacting VA's mission critical systems.

In response to our report, VA concurred with all findings and recommendations. The Assistant Secretary stated that action plans are currently being developed for each recommendation and detailed plans will be provided to the OIG in a separate response. The Assistant Secretary's response also stated that VA continues to make progress improving the effectiveness of its information security program. More specifically, VA's efforts have contributed to significant reductions in the number of outstanding plans of actions and milestones, a more effective risk assessment methodology, and improvements in privacy impact assessments for minor applications that hold sensitive data. The OIG will continue to evaluate VA's progress during the FY 2010 assessment.

CONCLUSION

Well publicized information security breaches at VA demonstrate that weaknesses in information security policies and practices can expose mission critical systems and data to unauthorized access and disclosure. While VA has made progress defining policies and procedures supporting its agency-wide information security program, its highly decentralized and complex system infrastructure poses significant challenges for implementing effective access controls, system interconnection controls, configuration management controls, and contingency planning practices that will adequately protect mission critical systems from unauthorized access, alteration, or destruction. Until VA fully implements key elements of its information security program and addresses our outstanding audit recommendations, VA's mission critical systems remain at an increased and unnecessary risk of attack or compromise.

Mr. Chairman, this concludes my statement. We would be happy to answer any questions you or other members of the Subcommittee may have.