STATEMENT OF
MICHAEL L. STALEY
ASSISTANT INSPECTOR GENERAL FOR AUDITING
OFFICE OF INSPECTOR GENERAL
DEPARTMENT OF VETERANS AFFAIRS
BEFORE
THE COMMITTEE ON VETERANS' AFFAIRS
UNITED STATES HOUSE OF REPRESENTATIVES

JUNE 14, 2006

INTRODUCTION

Mr. Chairman and Members of the Committee, thank you for the opportunity to testify today concerning the Office of Inspector General's (OIG) reports addressing information security weaknesses in the Department of Veterans Affairs (VA) and VA's implementation of OIG recommendations. I will provide an overview of the OIG reports that have shown the need for continued improvements in addressing information security weaknesses in VA and the status of OIG recommendations for corrective action.

SUMMARY OF PAST OIG REPORTS

We have conducted a number of audits and evaluations on information management security and information technology (IT) systems that have shown the need for continued improvements in addressing security weaknesses. We have 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 Federal Information Security Management Act (FISMA) audits have identified significant information security vulnerabilities since FY 2001. We continue to report security weaknesses and vulnerabilities at VA health care facilities and VA regional offices where security issues were evaluated during our Combined Assessment Program (CAP) reviews. We have also included IT security as a major management challenge for the Department in all required major management challenges reports issued from FY 2000 to the present.

Consolidated Financial Statement Audits Continue to Report Information Security as a Material Weakness

Pursuant to the Chief Financial Officers Act of 1990, the VA consolidated financial statements are audited annually. We contract with an independent public accounting firm to perform this audit. The contractor follows Government Accountability Office methodology to assess the effectiveness of computer controls at VA's three information technology centers (ITCs) and selected regional offices and medical centers.

As part of the CFS audit, IT security controls have been reported as a material weakness for many years. A material weakness is defined as a weakness in internal control that could have a material effect on the financial statements and not be detected by employees in the normal course of their business. We have reported that VA's program and financial data are at risk due to serious problems related to VA's control and oversight of access to its information systems. For

example, by not controlling and monitoring employee access, not restricting users to only need-to-know data, and not timely terminating accounts upon employee departure, VA has not mitigated the potential risk. These conditions place sensitive information, including financial data and sensitive veteran medical and benefit information, at risk, possibly without detection of inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

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 IT internal controls. We also recommended that VA continue its efforts to accomplish the following key tasks:

- Improve access control policies and procedures for configuring security settings on operating systems, improve administration of user access, and detect and resolve potential access violations.
- Evaluate user functional access needs and system access privileges to support proper segregation of duties within financial applications. Assign, communicate, and coordinate responsibility for enforcing and monitoring such controls consistently throughout VA.
- Develop a service continuity plan at the departmental level that will facilitate effective communication and implementation of overall guidance and standards, and provide coordination of VA's service continuity effort. Schedule and adequately test IT disaster recovery plans to ensure continuity of operations in the event of a disruption of service.
- Develop a change control framework and, within that framework, implement application specific change control procedures for mission critical systems.

VA has implemented some recommendations for specific locations identified but has not made corrections VA-wide. For example, we found violations of password policies which management immediately corrected, but in following years, we found similar violations at other facilities. We also found instances of terminated or separated employees with access to critical systems identified at various locations which management corrected, only to discover similar instances elsewhere.

Annual Evaluations of VA's Information Security Program Have Identified Vulnerabilities that Remain Uncorrected

FISMA requires us to annually review the progress of the information technology and security program of the Department and report the results to the Office of Management and Budget (OMB). As part of the FISMA review, we conduct scanning and penetration tests of selected VA systems to assess controls for monitoring and accessing systems, and reviews of physical, personnel, and electronic security. We visit the three major IT centers and selected regional offices and medical centers in addition to IT work on financial statements.

In all four audits of the VA Security Program issued since 2001, we reported vulnerabilities that continue to need management attention. These reports highlight specific vulnerabilities that can be exploited, but the recurring themes in these reports are the need for centralization, remediation, and accountability in VA information security. Since the FY 2001 report, we reported weaknesses in physical security, electronic security, and FISMA reporting, and since 2002, we also reported weaknesses in wireless security and personnel security. Additionally, we

have reported significant issues with implementation of security initiatives VA-wide. The status of unimplemented recommendations was discussed in subsequent audits.

The FY 2004 audit also emphasized the need to centralize the IT security program, implement security initiatives, and close security vulnerabilities. We previously recognized that the Office of the Assistant Secretary for Information and Technology/Chief Information Officer's (CIO's) office needed to be fully staffed, and that funding delays and resistance by offices to relinquish their own security functions and activities delayed implementation of the fully centralized CIO contemplated by our prior recommendations. The CIO's comments to the report referenced an April 2004 VA General Counsel opinion that held the CIO lacked the authority to enforce compliance with the VA information security program as one reason he could not address vulnerabilities. We again recommended that VA fully implement and fund a centralized VA-wide IT security program.

In total, the FY 2004 report included 16 recommendations: (1) centralize IT security programs; (2) implement an effective patch management program; (3) address security vulnerabilities of unauthorized access and misuse of sensitive information and data throughout VA demonstrated during OIG field testing; (4) ensure position descriptions contain proper data access classification; (5) obtain timely, complete background investigations; and complete the following security initiatives on (6) intrusion detection systems, (7) infrastructure protection actions, (8) data center contingency planning, (9) certification and accreditation of systems, (10) upgrading/terminating external connections, (11) improvement of configuration management, (12) moving VA Central Office (VACO) data center, (13) improvement of application program/operating system change controls, (14) limiting physical access to computer rooms, (15) wireless devices, and (16) electronic transmission of sensitive veteran data. As of June 9, 2006, all recommendations from this report remain open.

CAP Reviews Show Information System Security Vulnerabilities Continue to Exist

We continue to identify instances where out-based employees send veterans' medical information to the VA regional office via unencrypted e-mail; system access for separated employees is not terminated; monitoring remote network access and usage does not routinely occur; and off duty users' access to VA computer systems and sensitive information is not restricted. We continue to make recommendations to improve security and contingency plans, control access to information systems, complete background investigations and annual security awareness training, and improve physical security controls.

While individual and regional managers have concurred with these CAP recommendations, and our follow-up process confirms actions to resolve the specific conditions identified at these sites, we continue to find that corrective actions are not applied to all facilities to correct conditions nationwide. Consequently, we continue to find these systemic conditions at other sites we visit. For example, between FYs 2000 to 2005, the CAP program identified IT and security deficiencies in 141 (78 percent) of 181 Veterans Health Administration (VHA) facilities reviewed. We identified IT and security deficiencies at 37 (67 percent) of 55 Veterans Benefits Administration (VBA) facilities reviewed.

IT Security Remains a Major Management Challenge

The OIG annually summarizes the most serious management problems identified during reviews. We have identified information security and security of data and data systems in all major management challenge reports issued since FY 2000. The major management challenges are published in VA's annual Performance and Accountability Report.

STATUS OF CURRENT FISMA RECOMMENDATIONS

We have recently issued an advance copy our FY 2005 FISMA draft report to the Department. We restructured the draft report to respond to the Department's comments and announced reorganization actions designed to implement centralization in the CIO's office. While the OIG does not release draft reports, because of the extensive public interest in these issues resulting from the recent data loss incident involving the burglary of a VA data analyst's home, I would like to summarize the findings and recommendations of this report.

VA is still in the process of addressing recommendations made during prior FISMA audits to improve IT operations and controls. We have one additional recommendation for an existing area that needs to be elevated for priority attention. VA has made progress during FY 2005 to improve IT controls and to implement some recommendations. For example, after the FY 2005 testing was finished, VA informed us that certification and accreditation reviews have been completed and the deployment of intrusion detection systems (IDS) has been accomplished. We will validate implementation in future annual FISMA audits.

I will discuss in greater detail the 16 issues and discuss 1 new issue, as well as our recommendations for corrective actions.

Issue 1: Implementation of a Centralized Agency-wide IT Security Program

The CIO is VA's focal point for IT topics. Although the CIO is responsible for VA's information systems, operational controls were decentralized among each administration within VA. The operational control was, until recently, vested with VHA, VBA, National Cemetery Administration (NCA), and other program offices in VA. The CIO provided guidance and the tools to support the activities with operational control to secure VA systems, but the CIO did not have the ability to enforce or hold officials accountable for non-compliance. The CIO was responsible for the general management of all VA IT resources, including policy guidance, budgetary review, and general oversight. However, the implementation of the information security program was accomplished by VA personnel who were not under the direct supervision or control of the CIO.

Recently, Congress gave VA and the CIO a unique opportunity to centralize IT operational and maintenance activities, and to establish and implement policies designed to standardize IT functionality within the Department. For example, the House in November 2005 passed H.R. 4061, known as the *"Department of Veterans Affairs Information Technology Management Improvement Act of 2005."* This bill would give the VA CIO the authority to centralize IT operations and activities consistent with one of our open recommendations.

VA informed Congress that it plans to move towards a "federated IT system" to realign department-wide IT operations and maintenance responsibilities under the direct authority of the CIO. The main feature of the realignment will place VA's IT budget, along with IT professionals involved in operation and maintenance work, directly under the authority of the Assistant Secretary for Information and Technology/CIO. However, IT employees involved in system development will remain under their respective administrations and staff offices (e.g., VHA, VBA, NCA, and some program offices). Given that the planned realignment has just begun, VA's "federated IT system" implementation plans will need further study. For example, we will need to review whether existing IT systems and operations under the purview of the CIO will efficiently and effectively communicate with newly designed applications implemented by these system development offices. Failure to implement sound policies and procedures could introduce a significant amount of risk into the production environment if the access controls given to development staffs are not adequately developed and enforced.

Issue 2: Implementation of a Patch Management Program

VA continues to review and address patch management issues to find long-term solutions. We previously identified a number of critical patches that were either not installed or not appropriately implemented at the VA facilities reviewed. VA did not have an enterprise-wide solution that could directly connect to over 250,000 points within VA. During our FY 2005 review, VA continued to evaluate solutions to remediate this condition. VA was still in the process of developing and fully deploying a patch management program.

VA's CIO identified roles and responsibilities to address VA Enterprise Patch Management processes and standard operating procedures. A January 7, 2005, memorandum, *Enterprise Patch Management,* signed by the CIO, details patch management roles, responsibilities, and special considerations. We are continuing to follow up on the efforts taken by VA to implement this recommendation in future audits.

Issue 3: Electronic Security

Our reviews conducted at new sites visited during FY 2005 found potential vulnerabilities that we previously identified relating to password controls, remote access, and securing critical files. Additionally, we continued to find security vulnerabilities related to the lack of segregation of duties; unsecured critical files, which could allow attackers access to password files; and inappropriate access through remote access software.

Our field work at facilities not previously visited in prior years found potential vulnerabilities warranting management attention. The reviews indicate that while managers at sites visited are addressing vulnerabilities identified during these reviews, sites not visited in prior years have not been advised that the vulnerabilities identified may be systemic in nature. VA needs a consistent approach at all of its facilities to effectively monitor networks and to use tools, such as electronic scanning, to proactively identify and correct security vulnerabilities.

Issue 4: Personnel Security

In FY 2005, we continued to find previously identified weaknesses related to position descriptions and training of VA employees and contractors. Sensitive position descriptions

needed better documentation. We found the sensitivity rating was inaccurate for some employee positions at facilities reviewed and that position descriptions needed to more specifically address the levels of access relative to the positions' duties and responsibilities.

Issue 5: Background Investigations

VA needs to ensure that employee and contractor background investigation requirements are adequately identified and addressed. In FY 2005, we identified instances where background investigations and reinvestigations were not initiated in a timely manner on employees and contractors, or were not initiated at all. We will follow up on this issue in future FISMA audits.

Issue 6: Deployment and Installation of Intrusion Detection Systems

Although much has been done, the VA's Office of Cyber and Information Security (OCIS) still needs to validate whether VA completed installation of IDS at all sites. Deploying and installing IDS is a key step in the process of securing VA data systems on a national basis. Implementation of IDS increases VA's ability to detect intrusions. OCIS advised us that an enterprise-wide IDS has been fully implemented. In addition, OCIS is researching the benefits of moving to Intrusion Prevention Systems in an effort to provide VA the capability to detect and prevent "attacks." We will be testing the effectiveness of the IDS system in future FISMA audits.

Issue 7: Infrastructure Protection Actions

VA needs to complete infrastructure planning efforts. During our FY 2004 audit, we found examples where the physical infrastructure had significant vulnerabilities and did not adequately protect data from potential destruction, manipulation, and inappropriate disclosure. During our FY 2005 field work, we found that VA was developing a Critical Infrastructure Protection Plan, and completed an identification and prioritization of critical information resources. We will review VA's progress in completing and implementing this plan in future FISMA audits.

Issue 8: Information Technology Centers' Continuity of Operations Plans

VA is making progress and had completed Continuity of Operations (COOP) plans but full testing needs to be done. VA has issued an Emergency Preparedness Directive/Handbook 0320 for the VACO's COOP. VA was developing a Master COOP for the entire VA, which will include all elements in the Central Office COOP. National Institute of Standards and Technology (NIST) 800-34, *"Contingency Planning Guide for Information Technology Systems,"* dated June 2002, recommends COOP testing should be accomplished at least annually. COOPs covering ITCs need to ensure capabilities exist to provide necessary operational support in the event of disasters.

Our field tests conducted in FY 2005 showed that the ITCs have completed these contingency plans, but that testing these plans needed to be jointly done among all program offices residing in the ITCs. After FY 2005 field work was completed, we learned that VBA-related hardware had been procured at one ITC to back-up data, and some independent testing has been performed. For example, VBA informed us that they recently conducted tests at their ITCs and performed disaster recovery exercises. While this is a step forward, joint collaborative testing by all tenant

offices within the ITCs (VHA, VBA, NCA, and other offices) would serve as a better gauge of determining the adequacy of responses. We will follow up on this issue in future FISMA audits.

Issue 9: Certification and Accreditation Process

During FY 2005 field work, we found that VA had placed a priority on the uncompleted Certification and Accreditation (C&A) process. The number of VA systems and major applications decreased from 678 in FY 2004 to 585 in FY 2005, as a result of VA combining applications or by removing previously reported systems that did not meet the NIST criteria. At the end of our field work in the summer of 2005, VA had not completed a C&A for all systems and major applications. The Secretary of Veterans Affairs had made it a priority to complete all C&A work by the end of August 2005, and in November 2005, VA reported to OMB that it had completed a C&A for all VA systems and major applications. We will follow up in future FISMA audits to ensure all C&A work has been done, that self-reported deficiencies have been identified and actions are underway to address them, and that there is documentation to support the C&A work.

Issue 10: Terminate/Upgrade External Connections

In prior audits, we reported security risks associated with the operation of uncertified Internet gateways. As of FY 2005, VA took actions to mitigate these risks by limiting the number of Internet gateways in order to improve control over access to VA systems.

Field work conducted in FY 2005 found that VA is still unable to determine if all extraneous external connections have been terminated. We are currently unsure of the extent VA and its affiliated and non-affiliated partners may be operating their own gateways.

We also found that the standard contract VA used to procure computers included as a standard feature, modem devices, which if retained in default settings could serve as access points for hackers attempting to gain entry into VA systems. A January 2005 OIG report on procurement of desktop modems prompted VA to amend its contract and to address the modem security vulnerabilities with all facilities. We have left this recommendation open and will be continuing to review this issue during future FISMA audits.

Issue 11: Configuration Management

Prior year audits have found instances where VA networks relied on old operating systems such as Windows 95 and Windows 98, which placed the VA networks at risk due to the lack of vendor support to upgrade security and other features. An unsupported operating system, whether desktop or production mainframe, exposes VA to potential security and operational risks, including operating system failure.

During FY 2005 field work, we found VBA had reduced the number of personal computers running Windows 95, but other aged computers must continue to operate due to special document scanners associated with The Imaging Management System (known as “TIMS”). We were told that these scanners and personal computers are expected to be replaced or retired during FY 2006, if funds are available. Additionally, OCIS confirmed VHA has not completed the conversion of 161 older operating systems. In order to mitigate the risks associated with the

older operating systems, VHA moved the devices to a virtual local area network configuration with restricted access. The System Configuration and Management Program continues to review this issue, however, actions are still pending completion; therefore, we will follow up on future audits.

Issue 12: Movement and Consolidation of VACO's Data Center

We previously reported that the VACO data center was located below ground level and experienced water damage twice in the last 10 years. VA reported the relocation of the VACO data center is in progress. In the interim, VA placed equipment in multiple locations throughout the Washington, D.C., metropolitan area until procurement and construction is completed at a new location. Even though progress has been made, our observations identified routers and switches that support VACO network backbone critical to their operations remain below ground level. We will follow up on this issue in future FISMA audits.

Issue 13: Application Program/Operating System Change Controls

VA change control policy does not provide uniform application development and change guidance for a wide range of new and legacy applications. Nationwide policy is necessary to facilitate consistent implementation and effective monitoring of system change controls for mission critical systems.

For example, we found changes to a mainframe operating system and supporting hardware were not supported by local management authorization. Additionally, we found instances where changes to the production environment were not adequately documented or approved for major applications and critical systems. Consequently, unauthorized changes could have adversely affected the production environment or lead to misuse without warning. We will continue to follow up on this issue in future FISMA audits.

Issue 14: Physical Access Controls

At previous sites visited, VA was attempting to make improvements to ensure adequate measures were implemented to secure veterans' information and provide a safe environment for employees and visitors. However, our facility reviews at new locations showed physical access controls still need improvement. For example, a number of facilities granted access to computer rooms to employees who did not have a need to be in the computer room to perform their job function, and some contractors did not have an escort while in the computer room. We will continue to follow up on this issue in future FISMA audits.

Issue 15: Wireless Security

VA is making progress in reducing wireless security vulnerabilities by securing its network from outside intrusion. Actions were taken to install an encryption wireless product that is designed to prohibit unauthorized users from accessing the network. However, our contractor penetration test showed some vulnerabilities in the wireless network could be used to view transmissions, including those containing patient data, and to gain access to systems residing on VA's internal networks. Despite improvements, VA's information systems remained at risk for unauthorized access or misuse of sensitive information.

Issue 16: Encrypting Sensitive Information on VA Networks

VA has stated that it was taking interim steps to improve transmission of protected and sensitive information over its networks as sensitive data continues to be transmitted in clear text on VA networks. VA informed us that installation of encryption capabilities on some of its older platforms would render the systems inefficient. VA was looking for solutions to establish controls to secure electronic protected health information. However, field tests conducted in FY 2005 continued to demonstrate the need to improve controls as our contractor's penetration test showed an intruder could successfully capture protected health information in unencrypted clear text from outside a VA network. Our site work also showed that unencrypted protected health information was vulnerable at other VHA facilities.

Issue 17: FISMA Reporting Database

FISMA establishes security requirements and requires VA to annually report vulnerabilities for systems and major applications. While VA is taking actions to address security vulnerabilities, we continue to identify weaknesses that require a centralized and coordinated effort to ensure corrective actions are taken to control access, to secure computer rooms, and to ensure facilities accurately report their security deficiencies that place VA information and data at risk.

The FISMA database[1] contains the self-assessment surveys of VA's major applications and systems. System and application deficiencies, as well as funded and unfunded remediation plans, are reported and stored in this database. Consequently, this database needs to accurately demonstrate the security posture of VA's systems and major applications. Also, it should accurately depict the risk of loss of the critical and sensitive information contained within these systems and major applications.

Comparisons of the sites visited to the entries in the FISMA database found that not all information was accurate or complete. Most inaccuracies involved reporting of the five levels of IT security program effectiveness outlined in the Federal Information Technology Security Assessment Framework. Additionally, facilities were not held accountable for information inaccuracies or incomplete data in the database. For example, fields requiring information pertaining to the amount of funding needed to correct deficiencies were incomplete. VA senior leadership needs this information to determine the costs to correct the conditions identified. With inaccurate or incomplete information in the FISMA database, VA senior leadership will not have a complete picture of VA's information security posture and the level of resources and funding needed to remediate security deficiencies.

[1] In FY 2006, the FISMA database became known as the Security Management and Reporting Tool (SMART) database.

RECOMMENDATIONS

We recommended that the Acting Assistant Secretary for Information and Technology/CIO, in conjunction with senior VA leadership, take actions to fully address all 17 issues summarized above.

CLOSING

In closing, I would like the Committee to know that reviews of VA's information security will remain a priority for the OIG until these issues are resolved. We remain committed to following up and continuing to assess the adequacy of IT controls with the resources that are available, and we will remain dedicated to the goal of protecting our Nation's veterans.

Mr. Chairman and Members of the Committee thank you again for this opportunity to provide you the status of our work. I am available to answer any questions.