STATEMENT OF
SONDRA F. MCCAULEY
DEPUTY ASSISTANT INSPECTOR GENERAL FOR AUDITS AND EVALUATIONS
OFFICE OF INSPECTOR GENERAL
DEPARTMENT OF VETERANS AFFAIRS
BEFORE THE
COMMITTEE ON VETERANS' AFFAIRS
UNITED STATES HOUSE OF REPRESENTATIVES
HEARING ON
"VA'S LONGSTANDING INFORMATION SECURITY WEAKNESSES ARE INCREASING PATIENT WAIT TIMES AND ALLOWING EXTENSIVE DATA MANIPULATION"
NOVEMBER 18, 2014

Mr. Chairman and Members of the Committee, thank you for the opportunity to discuss the Office of Inspector General's (OIG) work regarding VA's Office of Information and Technology's (OIT) management of its information security programs. Our statement today focuses on VA's effectiveness in implementing the configuration management controls, access controls, security management, and contingency planning necessary to protect its mission-critical systems from unauthorized access, alteration, or destruction. We base our conclusions on the OIG's past and ongoing audits of VA's information security program. We will also focus on the challenges VA faces overcoming several information security concerns not highlighted in previous years. I am accompanied by Mr. Michael Bowman, Director, OIG Information Technology and Security Audits Division.

BACKGROUND

Information Technology (IT) systems and networks are critical to support VA in carrying out its mission of providing medical care and benefits and services to veterans. Ensuring the secure operation of these systems and networks is essential, given the wide availability of hacking tools on the Internet and the advances in the effectiveness of attack technology. Lacking proper safeguards, the systems and networks are vulnerable to intrusions by groups seeking to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other systems. VA previously reported a security incident in which sensitive information was compromised, including personally identifiable information (PII), potentially exposing millions of veterans and their families to the loss of privacy, identity theft, and other financial crimes.

INFORMATION SECURITY

This year, for the 15th consecutive year, the OIG's independent contractors who perform the annual audit of VA's consolidated financial statements have identified IT security controls as a material weakness. This work supports our requirements to perform annual Federal Information Security Management Act (FISMA) assessments. FISMA requires agencies to develop, document, and implement agency-wide information security risk management programs and prepare annual reports. FISMA also requires that each year, the OIG assess the extent to which VA complies with

FISMA's information security requirements, information security standards developed by the National Institute of Standards and Technology, and annual reporting requirements from the Office of Management and Budget.

In March 2012, VA instituted the Continuous Readiness in Information Security Program (CRISP) to ensure continuous monitoring year-round and establish a team responsible for resolving the IT material weakness. As a result, in our report, *Federal Information Security Management Act Audit for Fiscal Year 2013* (May 29, 2014), we discussed more focused VA efforts to implement standardized information security controls across the enterprise. As part of the fiscal year (FY) 2014 Consolidated Financial Statement audit, we reported some additional improvements in VA's IT security management. However these improvements require time to be fully implemented across VA's large enterprise-wide infrastructure and to show evidence of their effectiveness. The improvements we noted are:

- VA has continued predictive scanning of its networks to facilitate identification of system and network vulnerabilities across its field offices.
- VA has used the IT Governance, Risk, and Compliance tool, implemented in August 2013, to improve the process for assessing, authorizing, and monitoring the security posture of the agency.
- VA has improved implementation of its role-based and security awareness training and contingency plan testing.
- VA has reduced the number of individuals with outdated background investigations.
- VA has ensured consistent compliance with *United States Government Configuration Baseline* standards across the enterprise.

Despite progress made, OIT was not fully effective in addressing systemic weaknesses or eliminating the material weakness identified in VA's information security program for FY 2014. We continue to see repeat information security deficiencies in type and risk level to our reported findings in prior years and an overall inconsistent implementation of the security program. Communication between OIT's CRISP team and VA site managers also needs improvement. We will issue our FY 2014 FISMA audit in the spring of 2015 and it will discuss control deficiencies in four key areas: configuration management controls, access controls, security management, and contingency planning controls.

Configuration Management Controls are designed to ensure critical systems have appropriate security baseline controls and up-to-date vulnerability patches implemented. However, we found:

- Systems, including key databases supporting various applications, were not timely patched or securely configured to mitigate known and unknown information security vulnerabilities.
- The financial management system uses an unsupported database with several known critical vulnerabilities that cannot be updated with security patches, thus

preventing the implementation of effective security controls. Performance and security weaknesses are inherent with older versions of the system software.
- Change control policy and procedures for authorizing, testing, and approving system changes were not consistently implemented for networks and mission-critical system hardware and software changes.
- Several VA organizations were sharing the same local networks as other tenants at VA medical facilities and data centers; however, the tenant systems were not under the control of the local VA sites and often had critical or high-level vulnerabilities that weakened the overall security posture of the VA sites.
- Formal processes were lacking to monitor, prevent installation of, and remove unauthorized application software on VA systems.

Access Controls are designed to ensure that password standards are consistently implemented across the enterprise and that user accounts are monitored to enforce minimal access privileges necessary for legitimate purposes and to eliminate conflicting roles. Our work to date shows that:

- Password standards were not consistently implemented and enforced across multiple VA systems, including the network domain, databases, and mission critical applications. In addition, multi-factor authentication for remote access had not been fully implemented across the agency.
- Inconsistent reviews of networks and application user access resulted in numerous generic, system, and inactive user accounts that were not removed or deactivated from the system, and users with access rights that were not appropriate.
- Proper completion of user access requests was not consistently performed to eliminate conflicting roles and enforce principles of least system privilege.
- Monitoring of access was lacking in the production environment for individuals with elevated application privileges for a major application.
- Identification, notification, and remediation of security incidents were not consistently implemented to ensure incidents were resolved timely. In addition, network security event logs were not consistently maintained or reviewed across all facilities.
- Unknown and unmonitored system interconnections continued to exist and sometimes lacked valid Interconnection Security Agreements and Memoranda of Understanding to govern access to VA networks.

Security Management is designed to ensure that system security controls are effectively monitored on an ongoing basis and system security risks are effectively remediated through corrective action plans or compensating controls. As part of the FY 2014 Consolidated Financial Statement audit, we reported:

- Security management documentation, including the Risk Assessments and System Security Plan, and Privacy Impact Assessments were outdated and did not accurately reflect the current system environment or Federal standards.
- Background reinvestigations were not performed timely or tracked effectively. In addition, personnel were not receiving the proper level of investigation for the sensitivity levels of their positions.

- Scheduled completion dates for Plans of Action and Milestones (POA&Ms) were updated without written justification and supporting documentation was not adequate to justify POA&M closures. VA has approximately 9,000 open POA&Ms in FY 2014 compared with 6,000 in FY 2013.
- VA did not effectively manage and monitor its systems hosted at a cloud service provider.

Contingency Planning Controls ensure that mission-critical systems and business processes can be restored in the event of a disaster or emergency. However, we determined that:

- Backup tapes were not encrypted prior to being sent to offsite storage at selected facilities and data centers.
- Contingency plans did not reflect the current operating environment. Specifically, contingency plans had not been updated to reflect changes in system boundaries, roles and responsibilities, and lessons learned from testing contingency plans.

We continue to identify significant technical weaknesses in databases, servers, and network devices that support transmitting sensitive information among VA Medical Centers, Data Centers, and VA Central Office. For FY 2014 we once again found deficiencies where control activities were not appropriately designed or operating effectively. It is particularly disconcerting that a significant number of vulnerabilities we identified at VA data centers are more than 5 years old. In addition, inconsistent application of vendor patches designed to address such weaknesses jeopardize the data integrity and confidentiality of VA's financial and sensitive information.

Moving forward, VA needs to complete implementation of an enterprise-wide information security program and improve its monitoring process to ensure controls are operating as intended at all facilities. The dispersed locations, the continued reorganization of VA business units, and the diversity in applications adversely affected facilities and management's ability to consistently remediate IT security deficiencies agency-wide. For example, VA's complex and dispersed financial system architecture results in a lack of common system security controls and inconsistent maintenance of IT mission-critical systems. Consequently, VA continues to be challenged by a lack of consistent and proactive enforcement of established policies and procedures throughout its geographically dispersed portfolio of legacy applications and newly implemented systems. In addition, VA lacks an effective and consistent corrective action process for identifying, coordinating, correcting, and monitoring known internal security vulnerabilities on databases, web applications, and networks infrastructures. Effective communication between VA management and the individual field offices is critically needed to notify the appropriate personnel of identified security deficiencies so that they can timely implement corrective actions.

We expect to include in the FY 2014 FISMA audit a number of recommendations that remain unaddressed from prior years. Specifically, our FY 2013 FISMA report included 30 recommendations plus 5 unresolved recommendations from prior years'

assessments for a total of 35 outstanding recommendations. While OIT has made some initial effort, it has not provided sufficient information to support closing the recommendations. Overall, we recommended that VA:

- Address security-related issues that contributed to the IT material weakness that continues to be reported as a result of the annual audit of VA's consolidated financial statements.
- Remediate high-risk system security issues in its POA&Ms.
- Establish effective processes for evaluating information security controls via continuous monitoring and vulnerability assessments.
- Implement effective automated mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and web application servers.
- Institute procedures to oversee contractor management of cloud-based systems, ensure OIG access to those systems, and ensure information security controls are adequate to protect sensitive VA systems and data.
- Conduct periodic reviews to minimize access by system users with incompatible roles, permissions in excess of required functional responsibilities, and excessive or unauthorized accounts.

EMERGING INFORMATION SECURITY CONCERNS AT VA

This year, VA faces the added challenge of overcoming several information security concerns not highlighted in previous years such as cloud computing and foreign hackers. As appropriate, we have pursued these issues as a part of our FY 2014 FISMA audit work.

System Assessment and Authorization Process

Our FISMA testing for FY 2014 revealed potentially systemic deficiencies related to VA's system assessment and authorization process. We note that VA is maintaining production systems with "Temporary Authorizations to Operate" that are not based on completed reviews of security authorization packages, in accordance with National Institute of Standards and Technology standards. As a result, VA lacks assurance that system security controls are operating effectively, which could expose veterans' sensitive data to potential loss, fraud, or abuse.

OIG Hotline Allegations

We received a number of allegations through the OIG Hotline regarding ineffective VA information security management and controls that we evaluated as part of our FISMA audit. Specifically:

- VA was hosting medical devices containing sensitive patient information that are not effectively protected from unauthorized access, as required by VA's Medical Device Isolation Architecture.
- VA was misrepresenting information in preparation for the FY 2014 FISMA audit and this effort was consuming excessive resources within OIT.

- A software defect caused the self-service eBenefits portal to inappropriately display veterans' PII to other system users.
- Certain VA Medical Centers were hosting unauthorized systems and networks placing sensitive VA data at risk of loss or inappropriate disclosure.

We are currently working to finalize our analysis of these issues. We will provide conclusive determinations as to the merits of the allegations in our FY 2014 narrative FISMA audit report.

Veterans Health Information Systems and Technology Architecture

We have not evaluated all application modules within the Veterans Health Information Systems and Technology Architecture (VistA) as part of our FISMA audit. VistA was designed to provide an integrated inpatient and outpatient electronic health record for VA patients and administrative tools to help VA deliver medical care to veterans. As part of FISMA, we review selected controls within VistA supporting financial transactions; however, we did not assess the scheduling portion of the system.

The effectiveness of this patient scheduling system came into question as part of our review of allegations regarding inaccurate veteran wait times at the Phoenix VA Healthcare System. In late April 2014, we learned that certain audit controls within VistA were not enabled, which limited our ability to determine whether any malicious manipulation of the VistA data occurred. At our request, VA enabled this audit trail capability at Phoenix and nationwide. Inadequate use of system audit trails appears to be a systemic issue within VA. Specifically, as part of our FY 2014 consolidated financial statement and FISMA audits, we found that security event logs were not consistently maintained or reviewed across VA facilities. By not enforcing consistent use of audit logs for all systems, unauthorized system access and use may go undetected, placing sensitive VA data at unnecessary risk.

To facilitate our review of patient wait times, we also requested that OIT discontinue deleting VistA accounts for former employees and instead place these accounts in a disabled state so that we can evaluate system use and scheduling data. OIT complied with these requests. It may take VA several years to deploy the new patient scheduling system currently under development. The OIG is committed to performing additional scrutiny of the functionality and data integrity of this system as part of future reviews.

Cloud Computing

In February 2013, we communicated concerns to VA regarding its intent to migrate its email systems to a cloud service provider. Specifically, VA moved 15,000 email user accounts to a cloud-based system as part of a pilot study and planned to migrate the remaining 600,000 email user accounts to the virtual cloud environment thereafter. As a result, VA email messages were planned to be hosted on a contractor-owned and operated system.

Upon OIG review of the underlying contract, we noted the contract did not require the cloud service provider to allow OIG access to VA systems and data stored at the contractor facilities. Consequently, the OIG would not have legal access to VA systems

and data needed for investigative and oversight purposes. Further, the contract terms would potentially compromise our efforts to ensure that annual FISMA requirements are met. The contract lacked requirements for the cloud service provider to segregate VA sensitive data from other customer data, potentially impeding OIG investigations and creating new information security weaknesses involving VA electronic data. VA planned to adopt a policy to delete cloud-hosted emails greater than 90 days old in an effort to save costs with the cloud-based contract. Email is integral to the manner in which VA conducts day-to-day business. As such, retention of emails is critical to support VA work, OIG investigations and oversight reviews, and to defend VA actions in the administrative and judicial appellate systems.

In April 2013, the OIG issued a memorandum to the then-Deputy Secretary Scott Gould requesting that VA cease further contracting to put VA data in the cloud until all mission requirements of the OIG, VA General Counsel, and other VA administrations were met. Further, we requested that VA users not delete any email from any VA system until record management systems are established providing a minimum retention period of 7 years. We requested that all cloud-based systems be assessed at a "high" impact risk level to ensure that VA sensitive data are physically and logically segregated from other customer data hosted on the same virtual computer platforms. After several discussions with VA senior leadership, the then-Deputy Secretary directed that OIT terminate the email cloud-based contract because of concerns regarding retention of emails raised primarily by the OIG, as well as by General Counsel.

Foreign Hackers

In June 2013, we met with OIT to discuss whether VA networks have been compromised by foreign nation-state sponsored cyber espionage groups. OIT disclosed that since 2010, multiple external espionage groups have infiltrated VA networks and are actively attacking systems throughout the enterprise. Furthermore, OIT revealed that an Active Directory Domain Controller had been compromised, allowing malicious intruders to move laterally throughout the VA network. OIT stated that after identifying the compromised system, it devoted significant resources for more than a year in efforts to eradicate this threat, including requiring password resets for all affected systems. OIT admits that certain threat groups may still have access to VA systems using unauthorized user accounts. As such, OIT is still actively monitoring VA networks for evidence of system compromises today. We understand the Committee has asked the GAO to review whether the risks associated with foreign hackers on the VA network still exist. To not duplicate oversight efforts, we did not perform the additional tests needed to assess these risks.

PII Transmission Over Unsecure Internet Connections

In March 2013, we reported that VA was transmitting sensitive data, including PII and internal network routing information, over an unencrypted telecommunications carrier network.[1] VA disclosed that personnel typically transfer unencrypted sensitive data, such as electronic health records and internal Internet protocol addresses, among

[1] *Review of Alleged Transmission of Sensitive VA Data Over Internet Connections (*March 6, 2013).

certain VA Medical Centers and Community-Based Outpatient Clinics using an unencrypted telecommunications carrier network. OIT acknowledged this practice and formally accepted the security risk of potentially losing or misusing the sensitive information exchanged.

These risks continue to exist across VA's enterprise. Despite concurring with our report findings and recommendations, VA has not implemented the technical configuration controls needed to ensure encryption of sensitive data in accordance with VA and Federal information security requirements. Without controls to encrypt the sensitive VA data transmitted, veterans' information may be vulnerable to interception and misuse by malicious users as it traverses unencrypted telecommunications carrier networks. Further, malicious users could obtain VA router information to identify and disrupt mission-critical systems essential to providing health care services to veterans.

CONCLUSION

Our work has demonstrated that VA continues to struggle to effectively secure its IT systems. Some improvements in information security management have been realized with the inception of CRISP. However, more work remains to be done. Until a proven process is in place to address the OIG's outstanding report recommendations and ensure control across the enterprise, the IT material weakness will stand and VA's mission-critical systems and sensitive veterans' data will remain at risk of attack or compromise. IT shortfalls mean not only exposure of millions of veterans to potential loss of privacy, identity theft, and other financial crimes, they also constitute poor financial stewardship of taxpayer dollars.

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