STATEMENT OF
LINDA A. HALLIDAY
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
"HOW SECURE IS VETERANS' PRIVATE INFORMATION?"
JUNE 4, 2013

Mr. Chairman and Members of the Subcommittee, thank you for the opportunity to discuss the Office of Inspector General's (OIG) work regarding the securing of veterans' private information by VA. I am accompanied by Ms. Sondra McCauley, Deputy Assistant Inspector General for Audits and Evaluations, and Mr. Michael Bowman, Director, OIG's Information Technology and Security Audits Division.

BACKGROUND

Secure systems and networks are integral to supporting the range of VA mission-critical programs and operations. Information technology (IT) safeguards are essential due to the wide availability of hacking tools on the internet and the advances in the effectiveness of attack technology. Lacking proper safeguards, IT systems are vulnerable to intrusions by groups seeking to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other systems. VA has at times been the victim of such malicious intent. In the past, VA has reported security incidents in which sensitive information has been lost or stolen, including personally identifiable information (PII), potentially exposing millions of Americans to the loss of privacy, identity theft, and other financial crimes. The need for an improved approach to information security is apparent, and one that senior VA leaders well recognize.

In response to the need to improve security controls, VA has made progress defining policies and procedures supporting its Department-wide information security program. However, VA continues to face significant challenges implementing effective access controls, configuration management controls, and contingency planning to protect mission-critical systems from unauthorized access, alteration, or destruction. VA has taken positive steps to safeguard personal and proprietary information used by VA employees and contractors. Key actions have included:

- Mandating cyber security and privacy awareness training to ensure that VA and contract employees are familiar with applicable laws, regulations, and policies.
- Reviewing the accuracy of position sensitivity level designations for VA and contract employees.

- Strengthening its policies and procedures for identifying and reporting incidents involving information management and security violations to ensure that the incidents are promptly and thoroughly investigated.
- Establishing a clear chain of command and accountability structure for information security.

These were good first steps toward improving information security; however, more needs to be done. Over recent years, the OIG has conducted a series of reviews to help VA overcome its information security challenges by identifying the underlying causes for VA's security vulnerabilities and deficiencies. These include our statutory work, reviews of complaints to the OIG Hotline, and proactive reviews of internal controls. Our report findings have disclosed a pattern of ineffective information security controls that expose VA's mission-critical systems and sensitive data to unnecessary risk. We believe our corresponding audit recommendations provide a roadmap for VA to improve the effectiveness of its information security program and safeguard the sensitive data needed to support delivery of benefits and services to our Nation's veterans.

STATUTORILY-REQUIRED REVIEWS

For more than 10 consecutive years, independent public accounting firms under contracts with the OIG identified information technology security controls as a material weakness as a result of their annual audits of VA's Consolidated Financial Statements. Work on these audits supports our 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 the annual reporting requirements from the Office of Management and Budget.

In the middle of FY 2012, while our annual FISMA assessment was ongoing, 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 our FISMA work progressed, we noted more focused VA efforts to implement standardized information security controls across the enterprise. We also saw improvements in role-based and security awareness training, contingency plan testing, reducing the number of outstanding Plans of Action and Milestones (POA&Ms), developing initial baseline configurations, reducing the number of IT individuals with outdated background investigations, and improving data center web application security. However, the CRISP initiative was not launched until March 2012 and the improved processes had not been implemented for an entire fiscal year with the opportunity to demonstrate sustained improvements in information security.

For FY 2012, we provided a draft report to VA for review and comments and we expect to issue our report in June 2013. The report will discuss control deficiencies in four key areas:

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.
- Baseline configurations, including implementation of the Federal Desktop Core Configuration, were not consistently implemented to mitigate significant system security risks and vulnerabilities across the facilities.
- Change control policy and procedures for authorizing, testing, and approval of system changes were not consistently implemented for the networks and mission critical system hardware and software changes.

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 FISMA assessment revealed 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 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 and/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.
- Lack of monitoring of access in the production environment for individuals with elevated application privileges for a major application.

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. We will report that:

- Security management documentation, including the risk assessments and System Security Plans, 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 POA&Ms were updated without written justification and supporting documentation was not adequate to justify POA&M closures.

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:

- Contingency plan documentation had not been updated to reflect lessons learned from the contingency and disaster recovery tests, and detailed recovery procedures for all system priority components had not been documented and/or did not reflect current operating conditions.
- Backup tapes were not encrypted prior to being sent to offsite storage at selected facilities and data centers.

More importantly, we continue to identify significant technical weaknesses in databases, servers, and network devices that support transmitting sensitive information among VA's Medical Centers, Data Centers, and VA Central Office. Many of these weaknesses are due to inconsistent enforcement of an agency-wide information security program across the enterprise and ineffective communication between VA management and the individual field offices. Therefore, VA needs to improve its monitoring process to ensure controls are operating as intended at all facilities and communicate security deficiencies to the appropriate personnel to implement corrective actions.

We have identified and reported deficiencies where control activities were not appropriately designed or operating effectively. 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 had resulted 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.

Our FY 2012 FISMA report will include 27 current recommendations to the Acting Assistant Secretary for Information and Technology for improving VA's information security program. The report also highlights five unresolved recommendations from prior years' assessments for a total of 32 outstanding recommendations. Overall, we are recommending that VA focus its efforts in the following areas:

- Addressing security-related issues that contributed to the IT material weakness reported in the FY 2012 audit of the Department's consolidated financial statements.
- Remediating high-risk system security issues in its Plans of Action and Milestones.
- Establishing effective processes for evaluating information security controls via continuous monitoring and vulnerability assessments.

We continue to evaluate VA's progress during our ongoing FY 2013 FISMA audit and acknowledge increased VA efforts to improve information security, but we are still identifying repeat deficiencies, albeit to a lesser extent. This fall, upon completion of our FY 2013 FISMA testing and related work, we will make a determination as to whether VA's improvement efforts are successful in overcoming the IT material weakness.

OTHER REPORTS RELATED TO INFORMATION SECURITY

Over the past 2 years, we have issued a series of audits and reviews that have identified VA's information security controls deficiencies. Our reports disclosed a number of issues, including ineffective management of systems interconnections and sensitive data exchanges, delayed contractor background investigations, and inadequate access controls that placed sensitive veterans' data at unnecessary risk.

Review of Alleged Transmission of Sensitive VA Data Over Internet Connections

In March 2013, we substantiated an allegation made through the OIG Hotline that VA was transmitting sensitive data, including PII and internal network routing information, over an unencrypted telecommunications carrier network. VA Office of Information Technology (OIT) personnel disclosed that VA typically transferred unencrypted sensitive data, such as electronic health records and internal internet protocol addresses, among certain VA Medical Centers and Community Based Outpatient Clinics using an unencrypted telecommunications carrier network. OIT management acknowledged this practice and formally accepted the security risk of potentially losing or misusing the sensitive information exchanged.

VA has not implemented technical configuration controls to ensure encryption of sensitive data despite 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.

VA acknowledged transmitting PII over privately segmented networks to support service to veterans. VA concurred with our recommendations to improve the protection of sensitive data transmitted over the unencrypted carrier networks and implement configuration controls to ensure encryption of such data. VA clarified that it employs an industry telecommunications carrier network to provide a segmented network for transmitting PII, but noted that these network links are not currently employing encryption controls to protect sensitive data.

VA did not agree with the assertion that PII and internal network routing information were being transmitted over unsecured internet connections. However, based on interviews with OIT personnel at VA Medical Centers as well as information provided by the OIG Hotline complainant, we maintain that PII and router information were being

transmitted unencrypted through a telecommunications carrier that also provided internet services to customers outside of VA. Nonetheless, we commend OIT for performing a review of the locations associated with the Hotline complaint and inspecting communication networks to ensure proper segmentation of VA networks from internet connections. We recognize that industry telecommunications carriers can segment data traffic from unsecured Web connections. However, we believe the risk remains that sensitive VA data and router information can be compromised when it is transmitted across unencrypted telecommunications carrier networks outside of VA's span of technical control. More specifically, the network alone does not provide encryption, integrity, or authentication protections for the transmission of sensitive data and such services may be vulnerable to denial of service or sniffing attacks by malicious users. The Assistant Secretary for Information and Technology acknowledged these information security risks by stating OIT will review technical network communications practices across the enterprise and take corrective actions without hesitation.

Audit of VA System Interconnections With Research and University Affiliates

In October 2012, we reported on the effectiveness of VA's management of network interconnections and sensitive data exchanges with its research and university affiliates. Our audit disclosed that VA has not consistently managed its systems interconnections and data exchanges with its external research and university affiliates. Despite Federal requirements, VA could not readily account for the various systems linkages and sharing arrangements. VA also could not provide an accurate inventory of the research data exchanged, where data was hosted, or the sensitivity levels. In numerous instances, we identified unsecured electronic and hardcopy research data at VA Medical Centers and co-located research facilities.

We determined that VA's data governance approach has been ineffective to ensure that research data exchanged is adequately controlled and protected throughout the data life cycle. VA and its research partners have not consistently instituted formal agreements requiring that hosting facilities implement controls commensurate with VA standards for protecting the sensitive data. The responsible Veterans Health Administration program office's decentralized approach to research data collection and oversight at a local level has not been effective to safeguard sensitive VA information. Because of these issues, VA data exchanged with its research partners was considered to be at risk of unauthorized access, loss, or disclosure.

VA has the opportunity to further serve veterans by supplying the patient and medical data needed to achieve advancements in medical research and health care services. However, providing such sensitive data through electronic or hard copy means without effective information security controls and oversight has left the data susceptible to unauthorized access, loss, or disclosure. Leaving hosting facilities responsible for data governance at the local level without coordinated involvement of all stakeholders has proven ineffective and improvements are needed.

Establishing formal information security agreements is one method of documenting data sharing agreements and ensuring that hosting facilities institute information security controls commensurate with VA standards. Further, a centralized data governance and

storage approach would ensure researchers effectively control and securely manage sensitive VA research information over the data life cycle. Such measures are key to protect veterans' PII and personal health information and promote continued advancements in medical research now and for the future. VA generally concurred with our report recommendations. VA is taking corrective actions, however, all recommendations remain open as full implementation has not occurred.

Review of Alleged Incomplete Installation of Encryption Software Licenses

In October 2012, we substantiated a Hotline allegation that OIT had not installed and activated an additional 100,000 licenses purchased in 2011. As of July 2012, OIT officials stated they had installed and activated only a small portion, about 65,000 (16 percent), of the total 400,000 licenses procured. OIT did not install and activate all of the licenses due to inadequate planning and management of the project. Specifically, OIT did not allow time to test the software to ensure compatibility with VA computers, ensure sufficient human resources were available to install the encryption software on VA computers, and adequately monitor the project to ensure encryption of all VA laptop and desktop computers.

As such, 335,000 (84 percent) of the total 400,000 licenses procured, totaling about $5.1 million in questioned costs, remained unused as of 2012. Given changes in VA technology since 2006, VA lacked assurance the remaining software licenses were compatible to meet encryption needs in the current computer environment. Further, because OIT did not install all 400,000 encryption software licenses on VA laptop and desktop computers, veterans' PII remained at risk of inadvertent or fraudulent access or use.

We recommended the Assistant Secretary for Information and Technology complete an assessment of the encryption software project to determine whether the software was compatible with VA's operating systems and still met VA needs. Based on the assessment, we recommended that VA terminate the project or develop a plan, including adequate human resources and project monitoring, to ensure installation and activation of the remaining encryption software licenses. The Assistant Secretary for Information and Technology concurred with our finding and recommendations and is taking steps to move forward with the software implementation.

Review of Alleged Delays in VA Contractor Background Investigations

In September 2012, we reported on the merits of a complaint regarding ineffective VA management of its contractor background investigations. We substantiated that VA could improve management of its contractor background investigations. Specifically, VA had a backlog of 3,000 contractor background investigations as of April 2012, despite process improvements and a reduction in pending cases in recent months. VA also inappropriately prohibited contractors from working on awarded contracts although VA policy only requires initiating, not fully completing, investigations before contractors could start work.

According to VA officials, delays occurred due to ineffective management within VA's program office which is responsible for initiating and adjudicating background

investigations; staff misunderstanding VA's personnel security requirements and investigative processes; and no effective centralized system to monitor progress in addressing the backlog. In the absence of a system linking contractors needing background investigations with underlying contracts, we could not determine whether VA unnecessarily paid for contractors not yet authorized to work on awarded contracts. Nonetheless, VA officials said the backlog adversely affected their ability to fully staff major IT initiatives.

Our report provided several recommendations for improving procedures to reduce the backlog of contractor background investigations and implementing a central case management system to monitor contractor status and associated costs during the background investigation process. VA generally concurred with our findings and recommendations and has reported corrective actions to address them.

Review of Alleged Mismanagement of the Systems To Drive Performance Project

In February 2012, we reported that VA's Office of Management did not effectively manage the Systems to Drive Performance (STDP) project. We substantiated that VA did not adequately protect sensitive VA information from unauthorized access and disclosure. Specifically, we determined that more than 20 system users had inappropriate access to sensitive STDP information. On a specific note, VA's National Data Systems Group did not consistently approve requests for user access. Furthermore, project managers did not report unauthorized access as a security event, as required by VA policy. Security deficiencies occurred because STDP project managers were not fully aware of VA's security requirements for system development and had not formalized user account management procedures. Inadequate Information Security Officer oversight also contributed to weaknesses in user account management and the failure to report the granting of excessive user rights as security violations. As a result, VA lacked assurance of adequate control and protection of sensitive STDP data.

VA concurred with our findings and recommendation to ensure that employees assigned to the STDP project receive the role-based security training needed to address the issues highlighted in the report. Additionally, VA agreed to assign an Information Security Officer to the project to ensure VA's information security requirements are met. Corrective actions have been taken and these recommendations are now closed.

Review of Alleged Unauthorized Access to VA Systems

In July 2011, we reported on the merits of an OIG Hotline allegation that certain contractors without proper security clearances gained unauthorized access to VA networks and Veterans Health Information System and Technology Architecture (VistA) systems at multiple VA medical facilities. Our review substantiated the allegation and found that contractors improperly used other employees' Virtual Private Network user accounts to gain unauthorized access to VA systems and networks. The review also substantiated that contractor personnel did not obtain appropriate background security clearances before gaining access to VA systems and networks. Contractors admitted to sharing two of their employees' user accounts to access VA networks on a number of

occasions for maintenance and monitoring of contractor systems. Further, contractors could not provide evidence that it readily initiated actions to terminate user accounts after the employee's separation date.

VA policy specifically prohibits the sharing of user accounts and requires the closing of user accounts as part of proper user account management. Further, VA policy requires VA personnel to regularly review user account access for inappropriate or unusual activity and take necessary actions. Contractors stated they did not fully understand VA's information security requirements regarding user account access and did not believe additional user accounts were needed. Additionally, VA did not actively monitor user account activity or readily communicate with contractors the need periodically to identify and terminate unnecessary user accounts. Without effective controls to prevent unauthorized access by contractors, VA information systems and sensitive veterans' data are vulnerable to increased risks of compromised availability, integrity, and confidentiality. The lack of individual accountability over user accounts provides ample opportunities to conceal malicious activity such as theft or misuse of veterans' data. VA concurred with our findings and recommendations. However, the report remains open because a key recommendation regarding contractor security controls and practices has not been implemented almost 2 years after we issued the report.

CONCLUSION

Well-publicized information security incidents at VA demonstrate that weaknesses in information security policies and practices expose mission-critical systems and data to unauthorized access and disclosure. Through its CRISP initiative, VA has strengthened its efforts to define policies and procedures supporting its agency-wide information security program. However, its highly decentralized and complex system infrastructure poses significant challenges to implementing effective access controls, system interconnection controls, configuration management controls, and contingency planning practices that 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 and sensitive veterans' data remain at 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.