Office of Inspector General, Department of Veterans Affairs
Report Required under P.L. 114-113, Cybersecurity Act of 2015
August 15, 2016
MCI # 2016-01949-CT-0099

Section 406 of P.L. 114-113, The Cybersecurity Act of 2015, requires the Office of Inspector General of agencies that maintain covered systems to submit to Congress a description of the agency's cybersecurity policies, procedures, practices and capabilities[1]. Specific, agency reporting requirements include:

(1) Logical access policies and procedures used to access covered systems;
(2) A description of logical access and multi-factor authentication controls used to govern access to systems by privileged users;
(3) Policies and procedures for conducting inventories of the software present on systems and the licenses associated with such software;
(4) A description of the agency's capability to monitor and detect exfiltration and other threats; and
(5) Policies and procedures for ensuring that external entities, including contractors, implement the information security management practices described above.

The reporting areas specified within the law are evaluated during our annual information security audits conducted in accordance with the Federal Information Security Modernization Act (FISMA). Accordingly, we have included a copy of our annual Fiscal Year (FY) 2015 FISMA audit report, which describes our results for each of the above reporting areas. Additionally, our FISMA report provides audit results for other security control areas that are critical for the successful implementation of VA's information security program.

LOGICAL ACCESS POLICIES AND PROCEDURES

Logical access policies define the correct use of logical access controls such as password standards and user permission settings designed to protect agency information systems and data. Logical access procedures define the specific controls that will be used to enforce logical access policies. Logical access policies and procedures are provided in VA Directive 6500, *Managing Information Security Risk: VA Information Security Program* and VA Handbook 6500, *Risk Management Framework for VA Information Systems, VA Information Security Program,* which established the foundation for VA's comprehensive information security and privacy program and its practices based on applicable National Institute of Standards and Technology Special Publications. VA Directive and Handbook 6510, *VA Identity and Access Management,* provides specific policies and procedures for logical access assurance levels, electronic authentication risk assessments, identity proofing, identity credential management, electronic signature, and access management.

In 2015, VA's Chief Information Officer formed an Enterprise Cybersecurity Strategy team that was charged with delivering an enterprise cybersecurity strategic plan; to

[1] A covered system is defined as national security systems and federal computer systems that provide access to personally identifiable information (PII).

include logical access controls. The plan was designed to help VA achieve transparency and accountability while securing veteran information. The team's scope included management of current cybersecurity efforts, as well as development and review of VA's cybersecurity requirements from desktop to software to network protection. To address ongoing system security weaknesses, VA launched a Continuous Readiness in Information Security Program (CRISP) in 2012. The program is intended to improve logical access controls, configuration management, contingency planning, and the security management of a large number of information technology systems and ensure continuous monitoring year-round. VA also established a CRISP core team to oversee this initiative and resolve the information security material weakness related to information technology security controls, as reported in VA's annual audit of its consolidated financial statements. Overall CRISP goals are to support VA enterprise cybersecurity strategic plan, ensure compliance with VA information security requirements, and to assist facilities with the remediation of FISMA information security findings on a continual basis.

OIG Evaluation of Logical Access Policies and Practices: Our FY 2015 FISMA audit identified several significant deficiencies related to VA's identity management and logical access controls. Specifically, we identified: (1) a significant number of weak passwords on major databases, applications, and networking devices at most VA facilities; (2) numerous instances of unnecessary system privileges, excessive and unauthorized user accounts, and active accounts for terminated personnel; and (3) many VA facilities that did not have audit policy settings configured on major systems or had not implemented automated mechanisms needed to periodically monitor systems audit logs. More detail is included in our report.

LOGICAL ACCESS AND MULTI-FACTOR AUTHENTICATION CONTROLS

Logical access controls provide a technical means of controlling what information users can utilize, the applications that they can run, and the modifications they can make to systems and data. Multi-factor authentication controls are categorized by the number of factors that are incorporated into the user authentication process. The three factors considered as the cornerstone of multifactor authentication are: (1) something that you know such as a user password; (2) something that you have such as an identification badge or a cryptographic key; and (3) something that you are such as voice print or other biometric identification. According to an information security official, VA had implemented the following controls for logical access and multi-factor authentication controls. In January 2015, VA launched a phased implementation plan requiring full compliance by personnel for logical access via multi-factor authentication controls. In June 2016, VA began a phased implementation requiring two-factor authentication for local access and is working to meet Federal-wide targets for technical enforcement requiring the use of multi-factor authentication and the Personal Identity Verification card to access VA systems by both privileged user and non-privileged users. VA Handbook 6500 provides detailed procedures related to password management, system access management, capturing and maintaining audit trails, and remote access through multi-factor authentication.

OIG Evaluation of Logical Access and Multi-Factor Authentication Controls: Our FY 2015 FISMA audit noted that VA lacks a consistent process for managing remote access to VA networks and multi-factor authentication for remote access has not been fully implemented across the agency. Specifically, VA personnel can remotely log onto VA networks using several virtual private network applications for encrypted remote access. However, one specific application does not ensure end-user computers are updated with current system security patches and antivirus signatures before users remotely connect to VA networks. The FISMA report noted that VA needs to fully implement multi-factor authentication for remote access and ensure that all remote users' computers are adequately protected from secure locations before connecting to VA networks. More detail is included in our report.

SOFTWARE INVENTORY POLICIES AND PROCEDURES

According to an information security official, VA had implemented the following controls for software inventory policies and procedures. VA Directive 6403, *Software Asset Management Policy,* was approved in July 2015 and VA is implementing procedures in support of the Directive. For example, VA's Technology Innovation Program (TIP) office was recently established within the Office of Information and Technology (OIT) to support software asset management goals. The office is working to gather dispersed software asset data throughout VA. Below is a summary of specific procedures and training devised to implement the policy:

- VA employed a centralized software license management approach that is coordinated with key personnel for the majority of agency software license spending and enterprise wide licenses.
- The TIP office established a comprehensive SharePoint site that lists major software enterprise license agreements and many key attributes including costs, entitlement data, software product titles, and contract documentation. The SharePoint site is the foundation to employ a centralized license management approach across the agency.
- The TIP office developed software license agreement templates to guide key personnel for making informed software investment decisions and assist with the procurement of additional software enterprise license agreements as appropriate.
- The TIP office has worked with other VA program offices to identify software assessment management training needs.
- The TIP office has worked with information technology Workforce Development staff to develop a Web-based Software Asset management training course available through VA's Talent Management System.

OIG Evaluation of Software Inventory Policies and Procedures: Our FY 2015 FISMA audit noted that VA had not fully implemented the tools necessary to inventory the software components supporting critical programs and operations. We reported that incomplete inventories of critical software components could hinder patch management processes and restoration of critical services in the event of a system disruption or disaster. In addition, our testing revealed that VA facilities had not made effective use

of these tools to actively monitor their networks for unauthorized software, hardware devices, and system configurations. More detail is included in our report.

CAPABILITY TO MONITOR AND DETECT CYBERSECURITY THREATS

According to an information security official, VA has implemented various controls which allow the Department to monitor and detect data exfiltration and other cyber security threats throughout the enterprise. Specific capabilities provided below cover data loss prevention, forensics, and digital rights management:

- **Data Loss Prevention Capabilities:** VA's network traffic is monitored by Trusted Internet Connection security components to include stateful firewalls, application firewalls, and mail security relays. VA has also implemented the Einstein network monitoring capabilities as part of the National Cybersecurity Protection System at each of the network gateways. The Einstein capability provides protection of agency information systems through the detection and prevention of suspected cybersecurity threats. Additionally, VA is actively deploying a capability that will inspect encrypted traffic as it passes through the network gateways to the Internet, business partners, and other government agencies. VA has also implemented Internet Protocol blocking of incoming remote access from certain foreign countries and blocking of all outbound encrypted traffic that is not destined for legitimate external Internet sites. However, VA has not fully implemented a comprehensive Data Loss Prevention solution to prevent the exfiltration of certain critical data on the network. Consequently, VA is currently evaluating security products that will identify and protect sensitive data.

- **Forensics and Visibility Capabilities:** VA's Network and Security Operations Center provides a variety of tools for forensic monitoring and analysis of VA computers in support cybersecurity incident response. These forensic capabilities provide the ability to investigate security breaches, analyze malware infections, and conduct root cause analysis based on cybersecurity threats. VA's forensic capabilities include the following:

  (1**) System snapshot** – a snapshot can be taken of computer endpoints capturing its state at any given point in time. This includes information such as logged on users, open network connections, running processes, open files, and system information.
  (2) **Memory analysis** – an image of physical memory can be captured to validate exploits and identify the presence of active malware on a system. Volatile data such as encryption keys, passwords, hidden rootkits, and other critical evidence that's lost when a machine is powered off can be collected remotely to support forensics.
  (3) **Malicious code analysis** – unknown or potentially malicious files found during investigations are analyzed to understand their behavior and purpose. This aids in developing attack signatures and threat mitigation strategies.

(4) **Live analysis** – analysts can securely examine and gather artifacts of interest from any running host over the network. This enables analysts to preserve vital evidence and quickly analyze systems for compromise.
(5) **Physical media analysis** – When an in depth investigation is necessary, analysts will have the machine's hard drive shipped for full forensic analysis. In some cases, the hard drive can be acquired over the network. A full disk analysis is the most comprehensive type of forensic examination that can uncover critical information pertaining to incidents and recover a timeline of activities that have occurred.
(6) **Encase Enterprise** – Encase software is deployed VA wide to enable analysts to review the majority of Windows and Linux systems on networks that are impacted by cybersecurity incidents.

- **Digital Rights Management Capabilities:** VA has not yet implemented a digital rights management solution. According to the Office of Management and Budget (OMB) Memo M-16-03, "Guidance on Federal Information Security and Privacy Management Requirements", the Director of OMB indicated that agencies will draw on the results of the 2015 Federal Chief Information Officer Cyber Sprint efforts and provide guidance for implementing a new cybersecurity shared services strategy. One of the services to be offered is a Digital Rights Management shared service capability which could enable a systematic approach to data-level protection across the Federal Government. VA plans to take advantage of this Digital Rights Management shared services capabilities as soon as OMB provides details about the plan and services.

OIG Evaluation of VA's Incident Handling Capability: Our FY 2015 FISMA report noted that VA does not monitor all external interconnections or internal network segments for malicious traffic or unauthorized system activity. More specifically, we noted that some local facilities had prevented VA's Network and Security Operations Center from periodically testing certain systems for security vulnerabilities. Consequently, VA's Network and Security Operations Center does not have a complete inventory of all locally hosted systems and must rely on local sites to identify those systems for testing. More detail is included in our report.

POLICY AND PROCEDURES FOR MONITORING EXTERNAL ENTITIES

According to an information security official, VA had implemented the following policy and procedures for monitoring external entities. VA policies and procedures for ensuring that external entities, including contractors, implement the information security management practices described above are specified in VA Handbook 6500.6, *Contracts Security,* and in VA Directive 6066 *Personal Health Information and Business Associate Agreements.* In addition, standard templates and contracts clauses are in place to invoke cybersecurity and privacy requirements for all external entities and contractors who handle sensitive VA Personal Identifiable Information.

OIG Evaluation of VA's Monitoring of External Organizations: Despite the policy and procedures stated above, our FY 2015 FISMA audit disclosed several deficiencies

related VA's contractor oversight activities. Specifically: (1) VA could not provide evidence that contractor system security controls were appropriate; (2) VA could not provide an inventory of contractor systems interfaces and interconnection agreements; and (3) VA did not have adequate controls for monitoring cloud computing systems hosted by external contractors. More detail is included in our report.

Distribution

VA Distribution

Office of the Secretary Veterans Health Administration Veterans Benefits Administration National Cemetery Administration Assistant Secretaries Office of General Counsel Office of Acquisition, Logistics, and Construction

Non-VA Distribution

House Committee on Veterans Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs and Related Agencies
House Committee on Oversight and Government Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
Government Accountability Office
Office of Management and Budget
Department of Homeland Security

This work product is available on our Web site at www.va.gov/oig.