VA Office of Inspector General

OFFICE OF AUDITS & EVALUATIONS

Department of Veterans Affairs

Federal Information Security Modernization Act Audit for Fiscal Year 2015

March 15, 2016
15-01957-100

ACRONYMS

BIA	Business Impact Analysis
CRISP	Continuous Readiness in Information Security Program
DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GRC	Governance Risk and Compliance
NIST	National Institute of Standards and Technology
NSOC	Network and Security Operations Center
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plans of Action and Milestones
SP	Special Publication
VA	Department of Veterans Affairs
VAMC	VA Medical Center

Highlights: VA's Federal Information Security Modernization Act Audit for Fiscal Year 2015

Why We Did This Audit

The Federal Information Security Modernization Act (FISMA) requires agency inspectors general to annually assess the effectiveness of agency information security programs and practices. The VA Office of Inspector General's fiscal year 2015 audit sought to determine whether VA's information security program complied with FISMA requirements and applicable National Institute for Standards and Technology guidelines. We contracted with the independent accounting firm CliftonLarsonAllen LLP to perform this audit.

What We Found

VA had made progress developing policies and procedures but still faced challenges implementing components of its agency-wide information security continuous monitoring and risk management program to meet FISMA requirements. While some improvements were noted, this FISMA audit continued to identify significant deficiencies related to access controls, configuration management controls, continuous monitoring controls, and service continuity practices designed to protect mission-critical systems.

Weaknesses in access and configuration management controls resulted from VA not fully implementing security control standards on all servers, databases, and network devices. VA also had not effectively implemented procedures to identify and remedy system security vulnerabilities on network devices, database, and server platforms VA-wide.

Furthermore, VA had not fixed approximately 9,500 outstanding system security risks in its corresponding Plans of Action and Milestones to improve its information security posture. As a result, the fiscal year 2015 consolidated financial statement audit concluded that a material weakness still existed in VA's information security program.

What We Recommended

This report contains 35 recommendations for improving VA's information security program. We recommended the Assistant Secretary for Information and Technology implement comprehensive measures to mitigate security vulnerabilities affecting VA's mission-critical systems.

Agency Comments

The Assistant Secretary for Information and Technology agreed with our findings and recommendations. We will monitor the implementation of corrective action plans.

Brent E. Arronte

BRENT E. ARRONTE
Deputy Inspector General
for Audits and Evaluations

Table of Contents

DEPARTMENT OF VETERANS AFFAIRS

Memorandum

Date: February 18, 2016

From: Acting Assistant Inspector General for Audits and Evaluations

Subj: VA's Federal Information Security Modernization Act Audit for Fiscal Year 2015

To: Assistant Secretary for Information and Technology

1. Enclosed is the final audit report, *Federal Information Security Modernization Act Audit for Fiscal Year 2015*. The VA Office of Inspector General (OIG) contracted with the independent public accounting firm, CliftonLarsonAllen LLP, to assess the Department of Veterans Affairs' (VA) information security program in accordance with the Federal Information Security Modernization Act (FISMA).

2. To ensure the adequacy and effectiveness of information security controls, FISMA requires agency program officials, chief information officers, and inspectors general to conduct annual reviews of the agency's information security program and report the results to the Department of Homeland Security (DHS). DHS uses these data to assist in its oversight responsibilities and to prepare an annual report to Congress on agency compliance with FISMA.

3. VA continues to face significant challenges in complying with the requirements of FISMA because of the nature and maturity of its information security program. To better achieve FISMA outcomes, VA will need to focus on several key areas including:

   - Addressing security-related issues that contributed to the information technology material weakness reported in the fiscal year 2015 audit of VA's consolidated financial statements.
   - Successfully correcting high-risk system security issues identified within its Plans of Action and Milestones.
   - Establishing effective processes for evaluating information security controls via continuous monitoring and security vulnerability assessments.

4. CliftonLarsonAllen LLP was contracted to perform the FISMA audit and is responsible for the findings and recommendations included in this report. VA OIG does not express an opinion on the effectiveness of VA's internal controls during fiscal year 2015. Our independent auditors will follow up on the outstanding recommendations and evaluate the adequacy of corrective actions during their fiscal year 2016 FISMA audit.

5. This report provides 35 recommendations for improving VA's information security program; 31 recommendations are included in the report body and 4 recommendations are provided in Appendix A. The Appendix addresses the status of prior-year recommendations not included in the report body and VA's plans for corrective action. Some recommendations were modified or not closed because relevant security policies and procedures were not finalized, or information security control deficiencies were repeated during the fiscal year 2015 FISMA audit. VA successfully closed 4 recommendations and we identified 6 new recommendations in fiscal year 2015.

6. The effect of these open recommendations will be considered in the fiscal year 2016 assessment of VA's information security posture. We remain concerned that continuing delays in implementing effective corrective actions to address these open recommendations can potentially contribute to reporting an information technology material weakness for this year's audit of VA's consolidated financial statements.

BRENT E. ARRONTE
Deputy Assistant Inspector General
for Audits and Evaluations

for
GARY K. ABE
Acting Assistant Inspector General
for Audits and Evaluations

CliftonLarsonAllen LLP
11710 Beltsville Drive, Suite 300
Calverton, MD 20705
301-931-2050 I fax 301-931-1710
www.cliftonlarsonallen.com

February 17, 2016

The Honorable Linda A. Halliday
Deputy Inspector General
Department of Veterans Affairs
810 Vermont Avenue, NW
Washington, DC 20420

Dear Ms. Halliday:

Attached is our report on the performance audit we conducted to evaluate the Department of Veterans Affairs' (VA) compliance with the Federal Information Security Management Act of 2002 (FISMA) for the federal fiscal year ending September 30, 2015 in accordance with guidelines issued by the United States Office of Management and Budget (OMB) and applicable National Institute for Standards and Technology (NIST) information security guidelines.

CliftonLarsonAllen LLP was contracted to perform the FISMA audit and is responsible for the findings and recommendations highlighted in the attached report. We conducted this performance audit in accordance with Government Auditing Standards developed by the Government Accountability Office. This is not an attestation level report as defined under the American Institute of Certified Public Accountants standards for attestation engagements. Our procedures were designed to respond to the FISMA-related questions outlined in the OMB template for the Inspectors General and evaluate VA's information security program's compliance with FISMA requirements and applicable NIST information security guidelines, as defined in our audit program. Based on our audit procedures, we conclude that VA continues to face significant challenges meeting the requirements of FISMA.

We have performed the FISMA performance audit, using procedures prepared by CliftonLarsonAllen LLP and approved by the Office of the Inspector General (OIG), during the period April 2015 through November 2015. Had other procedures been performed, or other systems subjected to testing, different findings, results, and recommendations might have been provided. The projection of any conclusions, based on our findings, to future periods is subject to the risk that changes made to the information security program or controls, or the failure to make needed changes to the system or controls may alter the validity of such conclusions.

We performed limited reviews of the findings, conclusions, and opinions expressed in this report that were related to the financial statement audit performed by

CliftonLarsonAllen LLP. The financial statement audit results have been combined with the FISMA performance audit findings. We do not provide an opinion regarding the results of the financial statement audit results. In addition to the findings and recommendations, our conclusions related to VA are contained within the OMB FISMA reporting template provided to the OIG in November 2015. The completion of the OMB FISMA reporting template was based on management's assertions and the results of our FISMA test procedures, while the OIG determined the status of the prior year recommendations with the support of CliftonLarsonAllen.

This report is intended solely for those on the distribution list on Appendix F, and is not intended to be and should not be used by anyone other than these specified parties.

Sincerely,

CliftonLarsonAllen LLP

Calverton, Maryland
February 17, 2016

INTRODUCTION

Objective

The objective of this audit was to determine the extent to which VA's information security program and practices complied with Federal Information Security Modernization Act (FISMA) requirements, Department of Homeland Security (DHS) reporting requirements, and applicable Office of Management and Budget (OMB) and National Institute for Standards and Technology (NIST) guidance. The VA Office of Inspector General (OIG) contracted with the independent accounting firm CliftonLarsonAllen LLP to perform the fiscal year (FY) 2015 FISMA audit.

Overview

Information security is a high-risk area Government-wide. Congress passed the E-Government Act of 2002 (Public Law 107-347) as amended[1] in an effort to strengthen Federal information security programs and practices. FISMA provides a comprehensive framework to ensure the effectiveness of security controls over information resources that support Federal operations and assets. Audit teams assessed VA's information security program through inquiries, observations, and tests of selected controls supporting 55 major applications and general support systems at 26 VA facilities. In FY 2015, the teams identified specific deficiencies in these areas:

1. Agency-Wide Security Management Program
2. Identity Management and Access Controls
3. Configuration Management Controls
4. System Development/Change Management Controls
5. Contingency Planning
6. Incident Response and Monitoring
7. Continuous Monitoring
8. Contractor Systems Oversight

This report contains a total of 35 recommendations, including 6 new recommendations, for improving VA's information security program. Thirty-one recommendations are included in the report body and 4 recommendations are described in Appendix A. The Appendix addresses the status of prior recommendations not included in the report body and VA's plans for corrective action. VA successfully closed 4 recommendations in FY 2015. The FY 2014 FISMA report provided 33 recommendations for improvement.

[1] *The Federal Information Security Modernization Act of 2014 - Amends the FISMA Act of 2002 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth authority for the Secretary of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems.*

RESULTS AND RECOMMENDATIONS

Finding 1 Agency-Wide Security Management Program

FISMA requires each Federal agency to develop, document, and implement an agency-wide information security and risk management program. VA has made progress developing, documenting, and distributing policies and procedures as part of its program. However, VA still faces challenges implementing components of its agency-wide information security risk management program to meet FISMA requirements. Consequently, this FISMA audit continued to identify significant deficiencies related to access controls, configuration management controls, change management controls, and service continuity practices designed to protect mission-critical systems from unauthorized access, alteration, or destruction.

Progress Made While Challenges Remained

In 2015, VA issued an updated 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 NIST Special Publications. In FY 2015, the VA's chief information officer formed an Enterprise Cybersecurity Strategy team that was charged with delivering an enterprise cybersecurity strategic plan. 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. The agency submitted an enterprise cybersecurity strategy to Congress on September 28, 2015—ahead of schedule.

OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, issued in October 2015, provides guidance for Federal agencies to meet the report requirements under FISMA. To address annual reporting requirements and ongoing system security weaknesses, VA launched a Continuous Readiness in Information Security Program (CRISP) in FY 2012. The program is intended to improve 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.

As part of the CRISP initiative, we noted continued improvements in FY 2015 related to:

- Improving the information security awareness training process
- Reducing the number of individuals with outdated background investigations
- Improving data center Web application security
- Continuing to implement an IT governance, risk, and compliance tool to improve processes for assessing, authorizing, and monitoring the security posture of VA systems

However, these controls take time to mature and show evidence of their effectiveness. Accordingly, we continue to identify information system security deficiencies similar in type and risk level to our findings in prior years and an overall inconsistent implementation of the security program. Moving forward, VA needs to ensure a proven process is in place across the agency. VA also needs to continue to address control deficiencies that exist in other areas across all VA locations. VA has continued to implement the new RiskVision Governance Risk and Compliance (GRC) tool for the purpose of enterprise-wide risk and security management. However, our FISMA audit identified deficiencies related to VA's overall security and risk management approach, Plans of Action and Milestones (POA&Ms), and system security documentation, which are discussed in the following sections. Each of these processes is essential for protecting VA's mission-critical systems through appropriate risk mitigation strategies.

Risk Management Strategy

VA has not fully developed and implemented components of its agency-wide information security risk management program to meet FISMA requirements. VA has established an enterprise risk management program; however, the policies, procedures, and documentation included in the program were not consistently implemented, or applied, across all VA locations and systems.

For example, a major application at the Health Eligibility Center did not have a formal authorization to operate on VA's networks, as required by policy. Risk assessments did not consider all known system security risks. At most locations tested, we noted that risk assessments did not always: a) identify recommended corrective actions for mitigating security risks; b) identify appropriate corrective actions for control weaknesses; or c) identify all significant threat sources, such as risks associated with devices and systems not managed by OI&T. Furthermore, security deficiencies identified by the internal Enterprise Risk Management group were not incorporated into VA's risk management framework and GRC tool in a timely manner.

NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle*

Approach, states that an agency's risk management framework should address risk from an organizational perspective, with the development of a comprehensive governance structure and organization-wide risk management strategy. VA has implemented a risk governance structure, including a Risk Management Governance Board and the GRC tool, to monitor system security risks and implement risk mitigation controls across the enterprise. However, this effort has not been consistently implemented enterprise-wide.

Plans of Action and Milestones

OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, defines management and reporting requirements for agency POA&Ms, including deficiency descriptions, remediation actions, required resources, and responsible parties. According to data available from VA's central reporting database, VA has approximately 9,500 open POA&Ms in FY 2015, as compared with 9,000 open corrective actions in FY 2014. POA&Ms identify which actions must be taken to remedy system security risks and improve VA's overall information security posture.

VA has made progress in updating POA&Ms in a timely manner across VA sites and systems. Despite these improvements, audit teams continue to identify deficiencies related to reporting, managing, and closing POA&Ms. For example, audit teams identified POA&Ms that lacked sufficient documentation to justify closure, action items that missed major milestones, POA&Ms that lacked sufficient detail to describe the control weakness or the corrective actions taken to close the findings, and items that were not updated to accurately reflect their current status. In addition, closed POA&Ms assigned to specific systems or entities within the GRC tool were reopened once a new "Authorization To Operate" was given to that system. This creates a significant amount of administrative overhead when monitoring the current status of valid system risks and makes it difficult for management to provide an accurate picture of the outstanding weaknesses identified on their systems at any given time.

POA&M deficiencies resulted from a lack of accountability for closing items and a lack of controls to ensure supporting documentation had been recorded in the GRC tool. More specifically, unclear responsibility for addressing POA&M records at the "local" or "regional" level continues to adversely affect remediation efforts across the enterprise. By failing to fully document and remedy significant system security risks in the near term, VA management cannot ensure that information security controls will adequately protect VA systems throughout their life cycles. Moreover, without sufficient documentation in the central database to justify closure of POA&Ms, VA cannot ensure that corresponding security risks have been fully mitigated.

System Security Plans and Privacy Impact Assessments

Audit teams continue to identify system security plans with inaccurate information regarding operational environments, including system interconnections, accreditation boundaries, control providers, and compensating information security controls. We also noted that Privacy Impact Assessments were not updated to reflect the accreditation boundary changes from a local site to a regional boundary and service line model. The Enterprise Operations - Service Lines and Customer Application system security plans were not updated to reflect NIST 800-53 Revision 4 controls, as this version of the GRC tool (RiskVision) did not provide the needed functionality to address the most recent NIST guidelines, including the new privacy controls.

Also, management did not ensure that the system security plans, including the Facility Compliance Reports, were fully completed, updated, and reflected the current operating environment. Because of deficiencies in this area, system owners may not fully identify relative boundaries, interdependencies, compensating information security controls, and security risks affecting mission-critical systems.

Recommendations

1. We recommended the Assistant Secretary for Information and Technology fully implement an agency-wide risk management governance structure, along with mechanisms to identify, monitor, and manage risks across the enterprise. *(This is a modified repeat recommendation from prior years.)*

2. We recommended the Assistant Secretary for Information and Technology formally authorize Health Eligibility Center systems to operate in accordance with VA information security standards. *(This is a new recommendation.)*

3. We recommended the Assistant Secretary for Information and Technology implement clear roles, responsibilities, and accountability for developing, maintaining, completing, and reporting Plans of Action and Milestones. *(This is a repeat recommendation from prior years.)*

4. We recommended the Assistant Secretary for Information and Technology implement mechanisms to ensure Plans of Action and Milestones are updated to accurately reflect current status information. *(This is a repeat recommendation from prior years.)*

5. We recommended the Assistant Secretary for Information and Technology implement mechanisms to ensure sufficient supporting documentation is captured in the central Governance Risk and

Compliance tool to justify closure of Plans of Action and Milestones. *(This is a repeat recommendation from last year.)*

6. We recommended the Assistant Secretary for Information and Technology implement improved processes to ensure that all identified weakness are incorporated into Governance Risk and Compliance tool, in a timely manner, and corresponding POA&Ms are developed to track corrective actions and remediation. *(This is a new recommendation.)*

7. We recommended the Assistant Secretary for Information and Technology implement system enhancements to the Governance Risk and Compliance tool to prevent the automatic re-opening of closed Plans of Action and Milestones and update Enterprise Operation's version of the tool to reflect NIST 800-53 Revision 4 controls. *(This is a new recommendation.)*

8. We recommended the Assistant Secretary for Information and Technology develop mechanisms to ensure system security plans reflect current operational environments, including accurate system interconnections, boundary, control, and ownership information. *(This is a repeat recommendation from last year.)*

9. We recommended the Assistant Secretary for Information and Technology implement improved processes for reviewing and updating key security documents such as risk assessments, privacy impact assessments, and security control assessments on an annual basis and ensure all required information accurately reflects the current environment. *(This is a repeat recommendation from last year.)*

Finding 2 Identity Management and Access Controls

Audit teams identified significant deficiencies in VA's identity management and access controls. VA Handbook 6500, Appendix F, provides comprehensive guidelines for authenticating users and protecting VA's critical systems from unauthorized access, alteration, or destruction. Our FISMA audit identified significant information security control deficiencies in these areas:

- Password Management
- Access Management
- Audit Trails
- Remote Access

Password Management

While VA Handbook 6500, Appendix F establishes password management standards for authenticating VA system users, our teams continued to identify multiple password management vulnerabilities. For example, we continued to find a significant number of weak passwords on major databases, applications, and networking devices at most VA facilities. Additionally, password parameter settings for network domains, databases, key financial applications, and servers were not consistently configured to enforce VA's password policy standards.

While some improvements have been made, we continue to identify security weaknesses that were not remedied from prior years. Many of these weaknesses can be attributed to VA's ineffective enforcement of its agency-wide information security risk management program and ineffective communication from senior management to the individual field offices. The use of weak passwords is a well-known security vulnerability that allows malicious users to easily gain unauthorized access to mission-critical systems.

Access Management

VA Handbook 6500, Appendix F details access management policies and procedures for VA's information systems. However, reviews of permission settings identified numerous instances of unnecessary system privileges, excessive and unauthorized user accounts, accounts without formal access authorizations, and active accounts for terminated personnel. User access requests were not consistently reviewed to eliminate conflicting roles and enforce segregation of duties principles.

Additionally, we noted inconsistent monitoring of access in production environments for individuals with excessive privileges within major applications. This occurred because VA has not implemented effective reviews to monitor for instances of unauthorized system access or excessive permissions. Periodic reviews are critical to restrict legitimate users to

specific systems, programs, and data and to prevent unauthorized access by both internal and external users. Unauthorized access to critical systems can leave sensitive data vulnerable to inappropriate modification or destruction.

Audit Trails

VA did not consistently review security violations and audit logs supporting mission-critical systems. VA Handbook 6500, Appendix F, provides high-level policy and procedures for collection and review of system audit logs. However, most VA facilities did not have audit policy settings configured on major systems and had not implemented automated mechanisms needed to periodically monitor systems audit logs. Audit log reviews are critical for security-related activities, such as determining individual accountability, reconstructing security events, detecting intruders, and identifying system performance issues. Moreover, we have identified and reported deficiencies with audit logging for more than 9 years in our annual FISMA reports.

Remote Access

Although progress has been made, VA lacks a consistent process for managing remote access to VA networks. Multi-factor authentication for remote access has not been fully implemented across the agency. VA Handbook 6500, Appendix F establishes high-level policy and procedures for managing remote connections. 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.

Although the remote connections are encrypted, end-user computers could be infected with malicious viruses or worms, which can easily spread to interconnected systems. VA is migrating most remote users to virtual private network solutions that will better protect end-user computers through automated system updates. Moving forward, 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.

Recommendations

10. We recommended the Assistant Secretary for Information and Technology implement mechanisms to enforce VA password policies and standards on all operating systems, databases, applications, and network devices. *(This is a repeat recommendation from prior years.)*

11. We recommended the Assistant Secretary for Information and Technology implement periodic access reviews to minimize access by system users with incompatible roles, permissions in excess of required functional responsibilities, and unauthorized accounts. *(This is a repeat recommendation from prior years.)*

12. We recommended the Assistant Secretary for Information and Technology enable system audit logs and conduct centralized reviews of security violations on mission-critical systems. *(This is a repeat recommendation from prior years.)*

13. We recommended the Assistant Secretary for Information and Technology fully implement two-factor authentication for all local and remote access methods throughout the agency. *(This is a repeat recommendation from prior years.)*

14. We recommended the Assistant Secretary for Information and Technology implement mechanisms to ensure all remote access computers have updated security patches and antivirus definitions prior to connecting to VA information systems. *(This is a repeat recommendation from prior years.)*

Finding 3 Configuration Management Controls

Audit teams continue to find significant deficiencies in configuration management controls designed to ensure VA's critical systems have appropriate security baselines and up-to-date vulnerability patches implemented. VA Handbook 6500, Appendix F provides high-level policy guidelines regarding mandatory configuration settings for information technology hardware, software, and firmware. However, during testing we identified unsecure Web application servers, excessive permissions on database platforms, a significant number of outdated and vulnerable third-party applications and operating system software, and a lack of common platform security standards across the enterprise.

Unsecure Web Applications

Audits of Web-based applications identified instances of VA data facilities hosting unsecure Web-based services that could allow malicious users to gain unauthorized access to VA information systems. NIST Special Publication 800-44, Version 2, *Guidelines on Securing Public Web Servers*, recommends that organizations implement appropriate security management practices and controls when maintaining and operating a secure Web server. Despite the guidelines, VA has not implemented effective controls to identify and remedy security weaknesses on its Web applications. VA has mitigated some information system security risks from the Internet through the use of network filtering appliances. However, VA's internal network remains susceptible to attack from malicious users, who could exploit vulnerabilities and gain unauthorized access to VA information systems.

Unsecure Database Applications

Database vulnerability assessments continue to identify a significant number of unsecure configuration settings that could allow any database user to gain unauthorized access to critical system information. NIST Special Publication 800-64, Revision 2, *Security Considerations in the Information System Development Life Cycle*, states that configuration management and control procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the information system. VA has not implemented effective controls to identify and remedy security weaknesses on databases hosting mission-critical applications. In addition, key VA financial management systems used outdated database technology that makes flaw remediation difficult and hinders the VA's ability to mitigate certain vulnerabilities. Unsecure database configuration settings could allow any database user to gain unauthorized access to critical systems information.

Application and System Software Vulnerabilities

Network vulnerability assessments again identified a significant number of outdated operating systems and vulnerable third-party applications that could allow unauthorized access to mission-critical systems and data. NIST Special Publication 800-40, Rev 3, *Guide to Enterprise Patch Management Technologies*, states an agency's patch and vulnerability management

program should be integrated with configuration management to ensure efficiency.

VA has not implemented effective controls to identify and remedy security weaknesses associated with outdated third-party applications and operating system software. Deficiencies in VA's patch and vulnerability management program could allow malicious users unauthorized access to mission-critical systems and data. By implementing a robust patch and vulnerability management program, VA could effectively remedy vulnerabilities identified in operating systems, databases, applications, and other network devices.

Unsecure Network Access Controls

Network vulnerability assessments identified weak network segmentation controls that could allow unauthorized access to mission-critical systems and data. For example, we identified numerous biomedical devices that were not properly protected behind VA's Medical Device Isolation Architecture local area networks. More specifically, VA has not implemented effective methodologies for monitoring medical devices on the general network and ensuring medical devices are segregated from the primary local area network and the Internet. NIST Special Publication 800-41, Revision 1, *Guidelines on Firewalls and Firewall Policy* recommends that organizations use multiple layers of firewalls to provide defense-in-depth protections and limit access at more granular levels within the network.

We also noted that several VA organizations shared the same local network at some medical centers and data centers; however, the systems were not under the common control of the local site. Specifically, some non OI&T-controlled networks had significant critical or high risk vulnerabilities that weaken the overall security posture of the site. By not implementing effective network segmentation controls for major applications and general support systems, VA is placing critical systems at unnecessary risk of unauthorized access.

Baseline Security Configurations

VA has developed guidelines to define agency-wide security configuration baselines for its major information system components. FISMA Section 3544 requires each agency to establish minimally acceptable system configuration requirements and ensure compliance. However, we noted that common platform security standards were not consistently implemented and monitored on all VA platforms. For example, testing at VA facilities revealed varying levels of compliance, ranging from 89 to 94 percent, with United States Government Configuration Baseline standards for end-user systems.

More specifically, we identified two VA facilities with compliance ratings under 90 percent when compared with Federal baseline standards. Testing also identified numerous network devices not configured to a common security configuration standard, resulting in default network services, excessive permissions, weak administrator passwords, or outdated versions

of the network operating system. VA has also not fully documented or approved security baseline deviations against the Defense Information Systems Agency's - *Security Technical Implementation Guide* for various system platforms. By not implementing consistent agency-wide configuration management standards for major applications and general support systems, VA is placing critical systems at unnecessary risk of unauthorized access, alteration, or destruction.

Recommendations

15. We recommended the Assistant Secretary for Information and Technology implement more effective automated mechanisms to continuously identify and remedy security deficiencies on VA's network infrastructure, database platforms, and Web application servers. *(This is a repeat recommendation from last year.)*

16. We recommended the Assistant Secretary for Information and Technology implement a more effective patch and vulnerability management program to address security deficiencies identified during our assessments of VA's Web applications, database platforms, network infrastructure, and work stations. *(This is a repeat recommendation from last year.)*

17. We recommended the Assistant Secretary for Information and Technology maintain complete and accurate baseline configurations and ensure all baselines are appropriately implemented and checked for compliance with established VA security standards. (*This is a modified repeat recommendation from last year.)*

18. We recommended the Assistant Secretary for Information and Technology implement improved network access controls to ensure medical devices and non-OI&T managed networks are appropriately segregated from general networks and mission-critical systems. (*This is a repeat recommendation from last year.)*

19. We recommended the Assistant Secretary for Information and Technology consolidate the security responsibilities for non-OI&T networks present under a common control for each site and ensure vulnerabilities are remedied in a timely manner. *(This is a modified repeat recommendation from last year.)*

Finding 4 System Development/Change Management Controls

VA has not fully implemented procedures to enforce standardized system development and change management controls for mission-critical systems. Our audit teams continued to find software changes to mission-critical systems and infrastructure network devices that did not follow standardized software change control procedures.

FISMA, Section 3544, requires the establishment of policies and procedures to ensure information security is addressed throughout the life cycle of each agency information system. VA Handbook 6500.5, *Incorporating Security and Privacy into the System Development Life Cycle*, also discusses integrating information security controls and privacy throughout the life-cycle of each system.

Audit teams found numerous test plans, test results, and approvals that were either incomplete or missing. Specifically, at 3 major data centers and 4 VA medical centers (VAMCs), we noted that the change management policies and procedures for authorizing, testing, and approving system changes were not consistently implemented for changes to mission-critical applications and networks. By not enforcing a standardized change control methodology, system development projects may be inconsistently developed, tested, and migrated into production, placing VA systems at risk of unauthorized or unintended software modifications.

Recommendation

20. We recommended the Assistant Secretary for Information and Technology implement procedures to enforce a standardized system development and change control framework that integrates information security throughout the life cycle of each system. *(This is a repeat recommendation from last year.)*

Finding 5 Contingency Planning

VA contingency plans still were not fully documented or reflective of current operating environments. VA Handbook 6500, Appendix F, establishes high-level policy and procedures for contingency planning and plan testing. Our audit found the contingency planning deficiencies described below.

- Some Information System Contingency Plans had not been updated to reflect detailed disaster recovery procedures for all system components or reflect current operating conditions. Specifically, contingency plans had not been updated to reflect changes in the system boundaries, roles and responsibilities, and did not clearly identify alternate processing and storage sites. Additionally, backup and detailed recovery procedures used to restore systems were not always documented in the plans. We identified these issues at nine VAMCs, two major data centers, and one contractor facility.
- Backup tapes for mission-critical systems were not encrypted prior to transporting data offsite for storage. We identified this issue at one major data center and two VAMCs. VA has identified the lack of backup tape encryption as a vulnerability and has developed a corrective action plan to encrypt backup tapes in FY 2015.
- Contingency plans were not tested for the capability to failover to alternate processing sites. In addition, the Health Eligibility Center had not identified an alternate processing site to restore critical systems in the event of a disaster or emergency. We identified this issue at one major data center, five VAMCs, and two other facilities.
- A Business Impact Analysis (BIA) was not performed for the Financial Management System, the Personnel and Accounting Integrated Data system, the Veterans Service Network, and the Burial Operations Support System/Automated Monument Application System. BIAs are critical in assisting management in determining the priority of business functions and processes.

Incomplete documentation of contingency and disaster recovery plans may impede timely restoration of services in the event of system disruption or disaster. Moreover, by not encrypting backup tapes, VA is at risk of potential data theft or unauthorized disclosure of sensitive data. In October 2011, VA implemented the Office of Information and Technology Annual Security Calendar requiring all Information System Contingency and Disaster Recovery Plans to be updated on an annual basis. However, some updated plans continue to have weaknesses similar to those identified in FYs 2012 and 2013.

Recommendations

21. We recommended the Assistant Secretary for Information and Technology implement processes to ensure information system contingency plans are updated with the required information. *(This is a repeat recommendation from last year.)*

22. We recommended the Assistant Secretary for Information and Technology develop and implement a process for ensuring the encryption of backup data prior to transferring the data offsite for storage. *(This is a repeat recommendation from prior years.)*

23. We recommended the Assistant Secretary for Information and Technology implement improved processes for the testing of contingency plans and failover capabilities for major applications and general support systems to ensure that critical components can be recovered at an alternate site in the event of a system failure or disaster. *(This is a new recommendation.)*

24. We recommended the Assistant Secretary for Information and Technology perform and document a Business Impact Analysis for all systems and incorporate the results into an overall strategy development effort for contingency planning. *(This is a new recommendation.)*

Finding 6 Incident Response and Monitoring

VA has made significant progress in relation to its overall incident response program and network protection and monitoring capabilities. Newly implemented and leveraged technology, additional procedures, and enhanced management awareness and emphasis have allowed VA to strengthen its incident response and network security program. However, deficiencies were noted in several areas, including the cyber security event response time, the incident response metrics, the network sensor coverage and vulnerability scan monitoring, as well as the data exfiltration safeguards.

VA does not monitor all external interconnections and internal network segments for malicious traffic or unauthorized systems access attempts. More specifically, some local facilities had stopped VA's Network and Security Operations Center from periodically testing certain systems for security vulnerabilities. Consequently, the Network and Security Operations Center did not have a complete inventory of all locally hosted systems and must rely on local sites to identify systems for testing. Ineffective monitoring of internal network segments could block VA from detecting and responding to intrusion attempts in a timely manner.

Our audit continued to identify numerous high-risk cyber security incidents, including malware infections that were not remedied in a timely manner. Specifically, we noted a high number of malware security incident tickets that took more than 30 days to remedy and close. While VA's performance had improved from the prior year, the process for tracking higher risk tickets remained inefficient for a large portion of FY 2015, and some cyber security incidents were not remedied. By contrast, NIST Special Publication 800-61, *Computer Security Incident Handling Guide*, provides examples of cyber security incident response times, ranging from 15 minutes to 4 hours, based on the criticality of the incidents.

The guide also recommends that organizations develop their own incident response times based on organizational needs and the criticality of resources affected by the security incidents. We noted that VA had developed and implemented a set of metrics and monitoring procedures to assist with responding to security incidents during the year. The new monitoring allowed VA to affect a significant downward trend in ticket closure times as the year progressed. However, this incident response metric monitoring process did not cover the first 8 months of the fiscal year.

FISMA, Section 3544, requires each agency to develop and implement an agency-wide information security program containing specific procedures for detecting, reporting, and responding to computer security incidents. Notwithstanding Federal requirements, we performed six unannounced scans of internal networks; however, not all scans were detected by the NSOC. Specifically, NSOC detected the source Internet Protocol address for only

two of the six locations that were tested. During our interviews, management disclosed that network sensors used to identify suspicious traffic in transit were not fully implemented across the enterprise, resulting in unidentified network vulnerability scanning activity.

The controls that detect and prevent data exfiltration, at the four Trusted Internet Connection gateways, need to be improved. During fieldwork audit, teams were able to exfiltrate data out of VA by creating a User Datagram Protocol - Virtual Private Network tunnel transferring 54 megabytes of data without detection, both from the NSOC and from a VAMC. VA has a project in place to address control weaknesses noted in its data exfiltration controls.

Recommendations

25. We recommended the Assistant Secretary for Information and Technology implement more effective agency-wide incident response procedures to ensure timely resolution of computer security incidents in accordance with VA set standards. (*This is a repeat recommendation from prior years*.)
26. We recommended the Assistant Secretary for Information and Technology identify all external network interconnections and implement improved processes for monitoring all VA internal networks, systems, and exchanges for unauthorized activity. *(This is a repeat recommendation from last year.)*
27. We recommended the Assistant Secretary for Information and Technology implement improved safeguards to prevent data exfiltration from VA networks. (*This is a new recommendation.*)

Finding 7 Continuous Monitoring

Although progress had been made, we found that VA lacked comprehensive continuous monitoring program to manage information security risks and operations across the enterprise. Deficiencies were noted in the process of monitoring and assessing system security controls as well as in the overall application of a standard VA patch and vulnerability management process to all devices on all VA networks.

In addition, an agency-wide process had not been implemented for identifying and removing unauthorized application software on agency systems. Moreover, VA had not fully developed a software inventory to identify the applications needed to support critical programs and operations. NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, outlines the importance of deploying automated mechanisms to detect unauthorized components and configurations within agency networks. VA had been working on implementing an enterprise-wide continuous monitoring solution for unauthorized software.

Security control assessments had been incorporated into the VA continuous monitoring program and were used as a tool to monitor and manage the control environment of VA systems. Assessments could be done by several groups within VA, but the primary responsibility for performing internal control assessments at each VA facility was with the local system's specific owner and information security officer. Due to a lack of education and training, the methodologies and results of these internal control assessments were inconsistent. Consequently, our audit teams were able to identify assessments that did not evaluate the effectiveness of controls in the systems' operating environment, as well as assessments that used insufficient supporting documentation. NIST Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* requires that assessments address the operating effectiveness of controls.

Because of inadequate VA monitoring procedures, our technical testing team continued to identify significant deficiencies with configuration management controls designed to protect mission-critical systems from unauthorized access, alteration, or destruction. For instance, our testing team identified unsecure Web application servers, excessive permissions on database platforms, a significant number of outdated third-party applications, and inconsistent platform security standards across the enterprise.

Our audit teams also consistently identified devices on VA networks that were not incorporated into the overall VA vulnerability and patch management process. Specifically, we identified devices that were neither visible to NSOC scanners, nor provided appropriate credentials to allow

scanning for security vulnerabilities on such devices. Without effectively monitoring device configurations, software, and applications installed on VA networks, malicious users could introduce potentially dangerous software or malware into the VA computing environment.

To better meet continuous monitoring requirements, VA's *Information Security Continuous Monitoring Concept of Operations* established a centralized, enterprise information technology framework designed to support operational security demands for protection of critical information. This framework was based on guidance from Continuous Monitoring Workgroup activities sponsored by the Department of Homeland Security and the Department of State. The Office of Cyber Security continued to develop and implement Continuous Monitoring processes to better protect VA systems. The goal of *Information Security Continuous Monitoring* was to examine the enterprise to develop a real-time analysis of actionable risks that could adversely affect mission-critical systems.

At the time of our audit, VA had improved systems and data security control protections by implementing certain technological solutions, such as the GRC central reporting and monitoring tool, secure remote access, application filtering, and portable storage device encryption. Furthermore, VA had deployed various software and configuration monitoring tools to VA facilities as part of its "Visibility to Server" and "Visibility to Desktop" initiatives. However, VA had not fully implemented the tools necessary to inventory the software components supporting critical programs and operations. Incomplete inventories of critical software components 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.

Recommendations

28. We recommended the Assistant Secretary for Information and Technology fully develop a comprehensive list of approved and unapproved software and implement continuous monitoring processes to identify and prevent the use of unauthorized software on agency devices. *(This is a repeat recommendation from prior years.)*

29. We recommended the Assistant Secretary for Information and Technology develop a comprehensive software inventory process to identify major and minor software applications used to support VA programs and operations. *(This is a repeat recommendation from prior years.)*

Finding 8 Contractor Systems Oversight

In FY 2015, VA did not fully implement contractor oversight procedures as required by FISMA. According to FISMA, Section 3544, an agency should ensure adequate information security for systems that support its operations, including those provided by another agency, contractor, or other source. In addition, VA Handbook 6500.6, *Contract Security*, provides detailed guidance on contractor systems oversight and the establishment of security requirements for all VA contracts involving sensitive VA information. In spite of these requirements, our audit disclosed several deficiencies in VA's contractor oversight activities in FY 2015. Specifically:

- VA did not provide evidence that contractor system security controls were appropriate.
- VA provided an annual inventory of contractor systems; however, system interfaces and interconnection agreements were not included.
- VA did not have adequate controls for monitoring cloud computing systems hosted by external contractors. Consequently, we identified numerous critical and high severity vulnerabilities on contractor networks due to unpatched, outdated operating systems, and applications and configuration not being set to minimize security risks.

Without implementing effective oversight mechanisms, VA could not ensure that contractor security controls adequately protect sensitive systems and data in accordance with its information security requirements.

Recommendations

30. We recommended the Assistant Secretary for Information and Technology implement procedures for overseeing contractor-managed cloud-based systems and ensuring information security controls adequately protect VA sensitive systems and data. *(This is a repeat recommendation from last year.)*

31. We recommended the Assistant Secretary for Information and Technology implement mechanisms for updating the Federal Information Security Modernization Act systems inventory, including contractor-managed systems and interfaces, and annually review the systems inventory for accuracy. *(This is a repeat recommendation from last year.)*

Summary of Response From the Assistant Secretary for Information Technology

The Assistant Secretary for Information and Technology concurred with the findings and recommendations provided in this report and prepared a response, which is presented in Appendix D. In general, management's comments and corrective action plans are responsive to the recommendations and provided sufficient plans and target completion dates. Within the comments, the Assistant Secretary for Information and Technology stated that VA has made progress developing policies and procedures but material weaknesses remain in several areas. The Assistant Secretary also stated that implemented changes are grounded on a strategic framework for success that spans three phases: Now, Near, and Future.

As part of this strategy, the Service Delivery and Engineering team completed key initiatives that included customer experience, field operations optimization, infrastructure operations optimization, service desk optimization, organization structure redesign, and operations process streamlining.

We will continue to evaluate VA's progress during our audit of VA's information security program in FY 2016. We remain concerned that continuing delays in implementing effective corrective actions by estimated completion dates to address these open recommendations can potentially contribute to reporting an information technology material weakness from this year's audit of VA's Consolidated Financial Statements.

Appendix A Status of Prior-Year Recommendations

Appendix A addresses the status of outstanding recommendations not included in the main report and VA's plans for corrective action. As noted in the table below, some recommendations remain in progress, with estimated completion dates still to be determined. The corrective actions outlined below are based on management assertions and results of our audit testing.

Table 1. Status of Prior-Year Recommendations

Number	Recommendation	Status (In Progress or Closed)	Estimated Completion	Corrective Actions
FY 2006–03	We recommended the Assistant Secretary for Information and Technology update all applicable position descriptions to better describe position sensitivity levels, and improve documentation of personnel records of "Rules of Behavior" and annual privacy training certifications.	In Progress	To Be Determined	VA Directive and Handbook 0710, *Personnel Suitability and Security Program*, documents will be updated. To ensure position descriptions better describe sensitivity levels and improve documentation of "Rules of Behavior" and annual privacy training certifications, VA will require the use of Office of Personnel Management's Position Designation System and Automated Tool to improve current processes. In FY 2015, we continued to identify exceptions during testing.
FY 2006–04	We recommended the Assistant Secretary for Information and Technology ensure appropriate levels of background investigations be completed for all personnel in a timely manner, implement processes to monitor and ensure timely reinvestigations on all applicable employees and contractors, and monitor the status of the requested investigations.	In Progress	To Be Determined	VA is implementing an onboarding solution that will establish appropriate business rules based on the position descriptions in order to conduct background investigations and reinvestigations. Exceptions related to timely background

Number	Recommendation	Status (In Progress or Closed)	Estimated Completion	Corrective Actions
				investigations continued to be identified during FY 2015 FISMA testing.
FY 2006–08	We recommended the Assistant Secretary for Information and Technology reduce wireless security vulnerabilities by ensuring sites have up-to-date mechanisms to protect against interception of wireless signals and unauthorized access to the network, and ensure the wireless network is segmented from the general network.	In Progress	To Be Determined	VA is replacing the legacy wireless networks with more robust and secure wireless networks, defining strict configuration guidelines and implementation plans. VA established the National Wireless Infrastructure Team to ensure all authorized VA wireless access points use a standard wireless network configuration. Potential rogue access points continued to be identified during FY 2015 FISMA testing.
FY 2006–09	We recommended the Assistant Secretary for Information and Technology identify and deploy solutions to encrypt sensitive data and resolve clear text protocol vulnerabilities.	In Progress	To Be Determined	VA has launched a GETVPN project to encrypt sensitive data transmitted over external and internal data circuits and resolve clear text protocol vulnerabilities. Clear text protocol vulnerabilities were identified during our FY 2015 FISMA testing.

Appendix B Background

On December 18, 2014 President Barack Obama signed the Federal Information Security Modernization Act (FISMA) into law, which amends the Federal Information Security Management Act of 2002 to: reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices; and set forth authority for the Secretary of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems.

FISMA provides a comprehensive framework for ensuring effective security controls over information resources supporting Federal operations and assets. The statute also provides a mechanism for improved oversight of Federal agency information security programs. FISMA requires each Federal agency to develop, document, and implement an agency-wide security program. Agency-wide security program plans are also to include procedures for responding to security incidents, and require each agency to notify Congress of a major security incident within seven days.

Federal agencies are to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by the agency. As specified in FISMA, the agency Chief Information Officer or senior official is to oversee the development and maintenance of security operations that continuously monitor and evaluate risks and threats.

FISMA also requires agency Inspectors General to assess the effectiveness of agency information security programs and practices. Guidance has been issued by OMB and by National Institute of Standards and Technology in its 800 series of Special Publications supporting FISMA implementation. In addition, Federal Information Processing Standards was issued to establish agency baseline security requirements.

OMB and DHS provide instructions to Federal agencies and Inspectors General for preparing annual FISMA reports. In October 2015, OMB issued Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*. The memorandum establishes current Administration information security priorities and also provides agencies with Fiscal Year 2015 and 2016 FISMA and Privacy Management reporting guidance. Federal agencies are to focus on implementing the Administration's three cybersecurity priorities: (1) Information Security Continuous Monitoring; (2) Identity Credential and Access Management; and (3) Anti-phishing and Malware Defense. To comply with the reporting requirements, agencies must carry out the following activities:

- Agencies must respond to security posture questions on a quarterly and annual basis.
- Chief Information Officers should submit monthly data through CyberScope, the FISMA reporting application.
- The Chief Information Officers must report to DHS on a quarterly basis, and Inspectors General and Senior Agency Officials for Privacy must report to DHS on an annual basis.
- Agencies must participate in CyberStat accountability sessions and agency interviews conducted by DHS, OMB, and the White House National Security Staff.

DHS reporting instructions also focus on performance metrics related to key control activities such as information security continuous monitoring, configuration management, identity and access management, incident response and reporting, risk management, security training, corrective actions, remote access management, contingency planning, and contractor systems.

In 2015, DHS's FISMA reporting guidance for Inspectors General was updated to remove the security capital planning controls and to include a maturity model to use in assessing the effectiveness of agencies' continuous monitoring programs. VA OIG contracted with the independent accounting firm CliftonLarsonAllen LLP to conduct the annual FISMA audit for FY 2015. VA OIG provided oversight of the contractor's performance.

Appendix C Scope and Methodology

The FISMA audit determines the extent to which VA's information security program complies with FISMA requirements and relevant guidelines. The audit team considered Federal Information Processing Standards and National Institute of Standards and Technology guidance during its audit. Audit procedures included reviewing policies and procedures, interviewing employees, reviewing and analyzing records, and reviewing supporting documentation. VA OIG provided oversight of the audit team's performance.

This year's work included evaluation of selected major applications and general support systems hosted at 26 VA facilities that support National Cemetery Administration, Veterans Benefits Administration, and Veterans Health Administration lines of business. The audit teams performed vulnerability tests and evaluated management, operational, technical, and application controls supporting major applications and general support systems.

In connection with the audit of VA's FY 2015 consolidated financial statements, CliftonLarsonAllen LLP evaluated general computer and application controls of VA's major financial management systems, following the Government Accountability Office's Federal Information System Controls Audit Manual methodology. Significant financial systems deficiencies identified during CliftonLarsonAllen's evaluation are included in this report.

Site Selections

In selecting VA facilities for testing, the audit teams considered the geographic region, size, and complexity of each hosting facility, as well as the criticality of systems hosted at the facility. In selecting VA facilities for testing, the audit teams considered the geographic region, size, and complexity of each hosting facility, as well as the criticality of systems hosted at the facility. Sites selected for testing are described in Table 2.

Table 2. Summary of Sites Selected for Testing

Facilities	City	State
VA Medical Facility	Asheville	NC
VA Health Eligibility Center	Atlanta	GA
Information Technology Center	Austin	TX
VA Financial Service Center	Austin	TX
VA Medical Facility	Biloxi	MS
VA Medical Facility	Boise	ID
VA Regional Office	Boise	ID
Terremark, Cloud Service Provider	Culpepper	VA
VA Medical Facility	Gainesville	FL
VA Medical Facility	Grand Junction	CO
VA Regional Office	Hartford	CT
VA Medical Facility	Las Vegas	NV
Information Technology Center	Hines	IL
VA Medical Facility	Leavenworth	KS
Network Security Operations Center	Martinsburg	WV
Capitol Regional Readiness Center	Martinsburg	WV
VA Medical Facility	Montgomery	AL
VA Medical Facility	Omaha	NE
Information Technology Center	Philadelphia	PA
Loan Guaranty Contractor Managed Facility	Plano	TX
National Cemetery Administration	Quantico	VA
VA Medical Facility	Salem	VA
VA Medical Facility	West Haven	CT
VA Medical Facility	Wichita	KS
VA Regional Office	Wichita	KS
VA Central Office	Washington	DC

Vulnerability audit procedures used automated scanning tools and validation procedures to identify high-risk common security vulnerabilities affecting mission-critical systems. In addition, vulnerability tests evaluated selected servers and work stations residing on the network infrastructure; databases hosting major applications; Web application servers providing Internet and Intranet services; and network devices, including wireless connections.

Government Standards

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix D Management Comments

Department of Veterans Affairs

Memorandum

Date: February 4, 2016

From: Assistant Secretary for Information and Technology (005)

Subj: Draft Audit Report: Federal Information Security Management Act (FISMA) Assessment for FY 2014

To: Acting Assistant Inspector General for Audits and Evaluations

1. VA appreciates the opportunity to respond to the Office Inspector General's (OIG) draft report, *Federal Information Security Management Act Audit for Fiscal Year 2015.* As the OIG's assessment has noted, VA has made progress in developing policies and procedures but material weaknesses remain in several areas.

2. Our efforts will be built upon the progress made in 2015; for example:

   - We established an Enterprise Cybersecurity Strategy Team (ECST) to identify and eliminate material weaknesses in eight domains within the Office of Information Technology.
   - We improved the Continuous Readiness in Information Security Program (CRISP) to eliminate material weaknesses.
   - We established the Enterprise Program Management Office (EPMO) which will serve as OI&Ts "control tower" to manage VA's IT investments in a way that maximizes value, minimizes risk, and ensures transparency while maintaining a continuous emphasis on placing the Veteran's needs in the center of every system we develop or maintain.
   - We developed a strategic framework for success by stabilizing and streamlining core processes.
   - Institutionalized new set of capabilities to drive improved outcomes.

3. The changes we have implemented are grounded on a strategic framework of success that spans three phases: Now, Near, and Future. As part of the strategy, the Service Delivery and Engineering team completed key initiatives that included customer experience, field operations optimization, infrastructure operations optimization, service desk optimization, organization structure redesign, and operations process streamlining. Going forward, critical new enterprise functions will drive our strategy into action. The strategy establishes five new enterprise

functions including program management office, account management, quality and compliance, data management, and strategic sourcing. Our approach to enterprise cyber security was our first step in an action-based transformation. We have already made progress by delivering a new cybersecurity strategy to Congress on September 28, 2015, creating a nation control center in Austin, TX and integrating the Chief Technical Officer to the OI&T team to name a few.

4. If you have any questions, feel free to contact me at (202)-461-6910 or have a member of your staff contact Mr. Brian Burns, Deputy Assistant Secretary for Information Security at (703) 588-1829.

(original signed by:)

LaVerne H. Council

Attachment

Attachment

Office of Information and Technology Comments to Draft OIG Report, "Federal Information Security Modernization Act Audit for FY 2015" OIG Recommendations and OIT Responses:

Recommendation 1: We recommended the Executive in Charge for Information and Technology fully develop policy to address Federal requirements and implement an agency-wide risk management governance structure, along with mechanisms to identify, monitor, and manage risks across the enterprise. (This is a repeat recommendation from prior years.)

OIT Response: Concur. VA Risk Management program is outlined in VA policy, including 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, both of which are modeled after National Institutes of Standards and Technology (NIST) requirements. VA policy is implemented through mandatory employee training (both at the time of initial employment and refreshed annually) provided via the Talent Management System (TMS) and the Certification Program Office (CPO). VA policy is further implemented through standard operating procedures (SOP), such as the Assessment and Authorization (A&A) SOP which standardizes business processes of VA's partners thereby reducing operational risks. VA policy is further implemented through automated Continuous Monitoring (CM) and routine Security Control Assessments.

The VA will continue to conduct a root cause analysis of the Risk Management processes and workflows to identify best practices and deficiencies, and will take corrective actions to improve these processes and workflows where any issues are identified. Furthermore, where current tools being utilized are found to not be providing the same fidelity of information the OIG is able to receive, the VA will take actions to refine the tool in order to close the gaps.

Recommendation 2: We recommended the Assistant Secretary for Information and Technology formally authorize Health Eligibility Center systems to operate in accordance with VA information security standards. (This is a new recommendation.)

OIT Response: Concur. The VA is reviewing FISMA systems that comprise the Health Eligibility Center in accordance with VA policy. This recommendation is specific to the Workload Reporting and Productivity (WRAP) system which currently has an Authority To Operate (ATO) that will expire on February 5, 2016. OI&T is working with its business partners to ensure that required Assessment and Authorization documentation is provided prior to a subsequent ATO review.

Recommendation 3: We recommended the Assistant Secretary for Information and Technology implement clear roles, responsibilities, and accountability for developing, maintaining, completing, and reporting Plans of Action and Milestones. (This is a repeat recommendation from prior years.)

OIT Response: Concur. Existing VA policy, including 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, provides Guidance for Preparing and Submitting Security Plans of Action and Milestones, defines roles and responsibilities, management and reporting requirements for agency Plans of Action and Milestones (POA&M), including deficiency descriptions, remediation actions, required resources, and responsible parties. This policy is consistent with OMB Memorandum M-02-01 and National Institutes of Standards and Technology (NIST) requirements. POA&M requirements are implemented via existing Standard Operating Procedures (SOP), including the Assessment and Authorization (A&A) SOP. In addition, the VA provides role-based training on these procedures upon initial assignment of the function as well as part of annual refresher training provided by the Certification Program Office (CPO). Furthermore, the VA implemented a singular repository for POA&M's and this tool is utilized by individuals at all stages of the PO&AM process to store and track

information crucial to managing the POA&M process. Finally, the VA implemented dashboard type reporting to monitor overall POA&M status across FISMA systems.

The VA will examine the existing allocation of roles and responsibilities related to POA&M management, then implement changes to further clarify these functions in an effort to improve overall execution of the functions, through policy changes and SOPs, and increased supervision of the POA&M process. In addition, the VA will re-train the workforce through mandatory training for primary, secondary and tertiary roles involved POA&M management. The VA will review existing POA&M workflows inherent within the primary POA&M management and tracking system, then implement improvements on an as needed basis.

Recommendation 4: We recommended the Assistant Secretary for Information and Technology implement mechanisms to ensure Plans of Action and Milestones are updated to accurately reflect current status information. (This is a repeat recommendation from prior years.)

OIT Response: Concur. Existing VA policy, including 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, provides Guidance for Preparing and Submitting Security Plans of Action and Milestones, defines the mechanisms required to ensure Plans of Action and Milestones (POA&M) are updated to accurately reflect current status. This policy is consistent with OMB Memorandum M-02-01 and National Institutes of Standards and Technology (NIST) requirements. POA&M requirements are implemented via existing Standard Operating Procedures (SOP), including the Assessment and Authorization (A&A) SOP. In addition, the VA provides role-based training on these procedures upon initial assignment of the function as well as part of annual refresher training provided by the Certification Program Office (CPO). Further, the VA implemented the GRC RiskVision tool to be the singular repository for POA&M's and this tool is used to manage the POA&M process. Finally, the VA implemented dashboard type reporting to monitor overall POA&M status across FISMA systems.

To further refine the above, and to improve the current mechanisms mandated to ensure POA&Ms are updated to accurately reflect current status information, the VA will examine the existing allocation of roles and responsibilities related to POA&M management, then implement changes to further clarify these functions in an effort to improve overall execution of said functions, through policy changes and SOPs. In addition, the VA will re-train the workforce through mandatory training for primary, secondary and tertiary roles involved POA&M management. The VA will review existing POA&M workflows inherent within the Governance Risk and Compliance tool and then implement improvements on an as needed basis.

Recommendation 5: We recommended the Assistant Secretary for Information and Technology implement mechanisms to ensure sufficient supporting documentation is captured in the central Governance Risk and Compliance tool to justify closure of Plans of Action and Milestones. (This is a repeat recommendation from last year.)

OIT Response: Concur. Existing VA policy, including 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, provides Guidance for Preparing and Submitting Security Plans of Action and Milestones, defines the mechanisms to ensure sufficient supporting documentation is captured in the central Governance Risk and Compliance (GRC) tool to justify closure of Plans of Action and Milestones (POA&M). This policy is consistent with OMB Memorandum M-02-01 and National Institutes of Standards and Technology (NIST) requirements. POA&M requirements are implemented via existing Standard Operating Procedures (SOP), including the Assessment and Authorization (A&A) SOP. In addition, the VA provides role-based training on these procedures upon initial assignment of the function as well as part of annual refresher training provided by the Certification Program Office (CPO). Further, the VA implemented the GRC RiskVision tool to be the singular repository for POA&M's and this tool is used to manage the POA&M process. Finally, the VA implemented dashboard type reporting to monitor overall POA&M status across FISMA systems.

To further refine the above, the VA will further clarify the mechanisms to ensure sufficient supporting documentation is captured in the central repository to justify closure of POA&Ms, and then implement changes to further clarify these functions in an effort to improve overall execution of the functions, through policy changes and SOPs. In addition, the VA will re-train the workforce through mandatory training for primary, secondary and tertiary roles involved in POA&M management. The VA will review existing POA&M workflows inherent within the GRC tool and then implement improvements on an as needed basis.

Recommendation 6: We recommended the Assistant Secretary for Information and Technology implement improved processes to ensure that all identified weakness are incorporated into Governance Risk and Compliance tool, in a timely manner, and corresponding POA&Ms are developed to track corrective actions and remediation. (This is a new recommendation.)

OIT Response: Concur. Existing VA policy, including 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, provides Guidance for Preparing and Submitting Security Plans of Action and Milestones, defines the process requirements necessary to ensure that identified weakness are incorporated into Governance Risk and Compliance (GRC) tool, in a timely manner, and corresponding Plans of Action and Milestones (POA&M) are developed to track corrective actions and remediation. This policy is consistent with OMB Memorandum M-02-01 and National Institutes of Standards and Technology (NIST) requirements. POA&M requirements are implemented via existing Standard Operating Procedures (SOP), including the Assessment and Authorization (A&A) SOP. In addition, the VA provides role-based training on these procedures upon initial assignment of the function as well as part of annual refresher training provided by the Certification Program Office (CPO). Further, the VA implemented the GRC RiskVision tool to be the singular repository for POA&M's and this tool is used to manage the POA&M process. Finally, the VA implemented dashboard type reporting to monitor overall POA&M status across FISMA systems.

To further refine the above, the VA will implement improvements to current processes to ensure that identified weakness are incorporated into GRC tool, in a timely manner, and corresponding POA&Ms are developed to track corrective actions and remediation's, then implement changes to further clarify these functions in an effort to improve overall execution of the functions, through policy changes and SOPs. In addition, the VA will re-train the workforce through mandatory training for primary, secondary and tertiary roles involved in POA&M management. The VA will review existing POA&M workflows inherent within the GRC tool and then implement improvements on an as needed basis.

Recommendation 7: We recommended the Assistant Secretary for Information and Technology implement system enhancements to the Governance Risk and Compliance tool to prevent the automatic re-opening of closed Plans of Action and Milestones and update Enterprise Operation's version of the tool to reflect NIST 800-53 Revision 4 controls. (This is a new recommendation.)

OIT Response: Concur. To improve operational activities and alignment of the two respective tools, VA is currently integrating the two separate versions of Risk Vision into one version, thereby allowing for uniform updates, alignment of operational workflows, and improved compliance with NIST 800-53 Revision 4.

Recommendation 8: We recommended the Assistant Secretary for Information and Technology develop mechanisms to ensure system security plans reflect current operational environments, including accurate system interconnections, boundary, control, and ownership information. (This is a repeat recommendation from last year.)

OIT Response: Concur. VA policy, including 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, outline the requirements for maintaining accreditation related documentation to ensure system security plans reflect current operational environments, including accurate system interconnections, boundary, control, and ownership information and these requirements

are compatible with National Institutes of Standards and Technology (NIST) requirements. In addition, the Governance Risk and Compliance (GRC) tool provides workflows and processes to automate the accreditation documentation development process, with standardized templates, workflows and automatic notifications. Existing VA Assessment and Authorization (A&A) process workflows are designed to routinely assess accreditation artifacts, including system security plans, risk assessments, privacy impact assessments, and security control assessments during Authority To Operate (ATO) issuance, or at minimum, on an annual basis. These workflows support the risk acceptance process used by the Designated Approving Authority (DAA) to accredit the system.

The VA is conducting an assessment of the current accreditation roles and responsibilities, with particular emphasis on the System Owner roles and the allocation of these roles across the Department, including recommended changes to enhance accountability and satisfactory fulfillment of the prescribed functions. In addition, the VA will be implementing new process changes to enhance current documentation development processes. These actions will be leveraged to improve the accuracy of the documentation to ensure it more appropriately depicts the operational environment of the specific system, while simultaneously ensuring consistency. Further, the VA will be enhancing the current documentation templates within the GRC tool to better support the development of up-to-date and more accurate documentation.

Recommendation 9: We recommended the Assistant Secretary for Information and Technology implement improved processes for reviewing and updating key security documents such as risk assessments, privacy impact assessments, and security control assessments on an annual basis and ensure all required information accurately reflects the current environment. (This is a repeat recommendation from last year.)

OIT Response: Concur. VA policy, including 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, outline the requirements for maintaining, reviewing and updating key security documents such as risk assessments, privacy impact assessments, and security control assessments and these requirements are compatible with National Institutes of Standards and Technology (NIST) requirements. In addition, the Governance Risk and Compliance (GRC) tool provides workflows and processes to automate the accreditation documentation development process, with standardized templates, workflows and automatic notifications. Existing VA Assessment and Authorization (A&A) process workflows are designed to routinely assess accreditation artifacts, including system security plans, risk assessments, privacy impact assessments, and security control assessments during Authority To Operate (ATO) issuance, or at minimum, on an annual basis. These workflows support the risk acceptance process used by the Designated Approving Authority (DAA) to accredit the system.

The VA will be implementing new process changes to enhance current documentation development processes and requirements associated with reviewing and updating key security documents such as risk assessments, privacy impact assessments, and security control assessments are addressed to enhance current procedures and resolve any identified gaps. These actions will be leveraged to improve the accuracy of the documentation to ensure it more appropriately depicts the operational environment of the specific system, while simultaneously ensuring consistency. Further, the VA will be enhancing the current documentation templates within the GRC tool to better support the development of up-to-date and more accurate documentation.

Recommendation 10: We recommended the Assistant Secretary for Information and Technology implement mechanisms to enforce VA password policies and standards on all operating systems, databases, applications, and network devices. (This is a repeat recommendation from prior years.)

OIT Response: Concur. VA has implemented a process for monitoring password policies via predictive scans and remediation processes on OI&T systems. Routine system scans are completed by the Network Security and Operations Center (NSOC). Results of the scans are provided to each region for follow-up and remediation of password weaknesses or deviations from password policies and standards.

VA has implemented strong factor authentication for system administrators (to eliminate passwords) VA has aggressively worked to reduce elevated privileges as well, with a reduction of about 250,000 (93%) of identified elevated privilege accounts in the past 6 months. Personal Identity Verification (PIV) only authentication is progressing with Veterans Benefits Administration (VBA) being enforced and additional users in Veterans Health Administration (VHA) enforced in Fiscal Year (FY) 2016. VA has initiated a single sign-on (SSO) program for external (SSOe) and internal (SSOi) users to verify applications require password in accordance with VA requirements. In 2016, VA will acquire additional password compliance tools. These tools are needed to interface Linux/Unix/Macs with Active Directory, which in turn enables these systems to be strong factor authentication compliant (i.e., ability to log on with a token instead of a password).

Recommendation 11: We recommended the Assistant Secretary for Information and Technology implement periodic access reviews to minimize access by system users with incompatible roles, permissions in excess of required functional responsibilities, and unauthorized accounts. (This is a repeat recommendation from prior years.)

OIT Response: Concur. A review of privileged access to VA information systems is completed on a quarterly basis. The Department has implemented periodic access reviews to minimize access by system users to track and manage status updates of access reviews that are issued. The VA requires users to request privileged access via the electronic Permissions Access System (ePAS). Using various systems monitoring tools and ePAS, Information Security Officers in conjunction with field operations staff and VA management, monitor privileged access to ensure users have proper authorization and least privilege to VA information systems. Furthermore, the Information Security Officers (ISOs) work to identify issues and concerns with staff elevated privileges and, when necessary, engage the user's supervisor for final determination and resolution. This on-going review process serves to minimize the number of system users with incompatible roles and permissions in excess of required functional responsibilities. A comprehensive review of remote access is done annually while a review of separated users from VA occurs every quarter. These reviews ensure that remote access is still required and authorized.

Recommendation 12: We recommended the Assistant Secretary for Information and Technology enable system audit logs and conduct centralized reviews of security violations on mission-critical systems. (This is a repeat recommendation from prior years.)

OIT Response: Concur. VA is continuing efforts to enhance the ability to centrally collect and monitor logs and correlate data throughout the enterprise. The VA Network Security and Operations Center expanded its existing log aggregation effort to a pilot within the regions to collect a sample of windows events logs. This provided a successful Proof of Concept for the implementation which will perform log collection and correlation. The solution has been procured and the project is proceeding as scheduled.

Recommendation 13: We recommended the Assistant Secretary for Information and Technology fully implement two-factor authentication for all local and remote access methods throughout the agency. (This is a repeat recommendation from prior years.)

OIT Response: Concur. In January 2015, VA implemented the phased implementation plan requiring full compliance by VA personnel. At present, two-factor authentication for remote access is 99% complete for Remote Enterprise Security Compliant Update Environment (RESCUE) Virtual Private Network (VPN) users by requiring the use of a Personal Identity Verification (PIV) card to authenticate at the gateway. Additional enhancements of two-factor authentication for Citrix Access Gateway (CAG) users are underway.

Recommendation 14: We recommended the Assistant Secretary for Information and Technology implement mechanisms to ensure all remote access computers have updated security patches and antivirus definitions prior to connecting to VA information systems. (This is a repeat recommendation from prior years.)

OIT Response: Concur. VA recommends that this OIG recommendation be closed. A summary of actions taken throughout 2014 and 2015 to resolve the finding include the following:

- Memorandum signed by the DAS for Information Security on February 4, 2014, specified elimination of the use of Personally Owned Equipment through any means other than Citrix.
- Memorandum signed by the DAS for Information Security calling for the full decommissioning of the One VA Virtual Production Network (VPN) solution on July 25, 2014.
- February 2015, audit checks and automated blocking mechanisms to meet the requirements in VA Handbook 6500, Risk Management Framework for VA Information Systems, VA Information Security Program, were implemented for Remote Enterprise Security Compliant Update Environment (RESCUE) and Secure Mobility Clients (SMC). This includes: Anti-Virus (AV) signature updates, critical (zero-day patch) patch compliance, Host Intrusion Prevention Software (HIPS), etc. Citrix is a virtual session between the client and the VA. Therefore, the client does not actually touch the VA network.

Recommendation 15: We recommended the Assistant Secretary for Information and Technology implement more effective automated mechanisms to continuously identify and remedy security deficiencies on VA's network infrastructure, database platforms, and Web application servers. (This is a repeat recommendation from last year.)

OIT Response: Concur. VA has an enterprise-wide scanning program performed by the Network Security and Operations Center (NSOC) on a scheduled basis. The NSOC conducts scans as needed or requested. Results of the scans are rolled into the process for analysis and reporting. The analysis tool provides an Enterprise view down to the terminal device level (specific Internet Protocol (IP)).

Recommendation 16: We recommended the Assistant Secretary for Information and Technology implement a more effective patch and vulnerability management program to address security deficiencies identified during our assessments of VA's Web applications, database platforms, network infrastructure, and work stations. (This is a repeat recommendation from last year.)

OIT Response: Concur. VA has implemented an enterprise-wide vulnerability management program that makes use of a number of scanning tools to identify security deficiencies; augmentation to incorporate the findings for a remediation warehouse, and an Enterprise view down to the terminal device level (specific IP). The Network Security and Operations Center (NSOC) has instituted database scanning during FY 2015 as well as Cisco credentialed device scanning and Red Hat Linux scanning. One-off scans occurred during FY 2015 in preparation for OIG visits with the capability of facilities doing their own validation scans ad hoc. VA, OI&T Information Security (OIS) and Service Delivery and Engineering (SDE) also engaged the Department of Homeland Security (DHS) to provide deeper penetration database scanning.

Recommendation 17: We recommended the Assistant Secretary for Information and Technology maintain complete and accurate baseline configurations and ensure all baselines are appropriately implemented and checked for compliance with established VA security standards. (This is a modified repeat recommendation from last year.)

OIT Response: Concur. VA has a process for baseline development and implementation. Current baselines cover the following categories: databases; operating systems; network devices. Technologies not covered by baselines are constantly being revisited so that baselines can be created for those technologies. In FY 2015, an effort was initiated to implement the Structured Query Language (SQL) 2012 baseline. Baselines encompass system hardening, Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), United States Government Configuration Baseline (USGCB) settings. Several reporting tools are available and are in the process of being utilized. VA, OI&T Information Security (OIS), Network Security and Operations Center (NSOC) and Service Delivery and Engineering (SDE) are engaged in a current effort to develop additional baseline compliance reports.

Recommendation 18: We recommended the Assistant Secretary for Information and Technology implement improved network access controls to ensure medical devices and non-OI&T managed

networks are appropriately segregated from general networks and mission-critical systems. (This is a repeat recommendation from last year.)

OIT Response: Concur. A Medical device is defined as any device that meets the following requirements:

- If the device is used in patient healthcare for diagnoses, treatment (therapeutic), monitoring physiological measurements, or for health analytical purposes or,
- If the device has gone through the Federal Drug Administration's (FDA) Premarket Review Process (510K Certification) or,
- If the device is incorporated as part of a medical system and, if modified, can have a negative impact on the functionality/safety of the main medical system
- Medical devices and clinical systems are listed in the VA-Medical Device Nomenclature System naming standard and shall be located on the Medical Device Isolation Architecture and follow the policies applicable to medical devices per the Medical Device Protection Program.

Non-OI&T managed networks:

- Facility Critical Infrastructure Systems include but are not limited to environmental controls, emergency management, police surveillance systems; physical access control systems connected to the VA network.
- Tenant Networks at VA facilities (OI&T Managed) are OI&T managed networks, segregated from local facility networks, and are managed by another OI&T office, not supporting the local facility. (examples include: Veterans Canteen Cash Register Systems; ESE domain controller enclaves; VBA laptops/workstations at VHA facilities)
- Tenant Networks at VA facilities (non-OI&T Managed) are network enclaves on local facility networks that are not managed by OI&T staff and most likely managed by the business office, contracted support or other non OI&T support.

VA has an existing Medical Device Protection Program (MDPP) that provides security for networked connected medical devices. The existing security architecture in place at the VA has been enhanced with the following items that are in progress or recently completed to support the cyber security of network connected medical devices. Due to the shared risk responsibility that VHA has with the medical device manufacturers, the isolation of network connected medical devices in Virtual Local Area Networks (VLANs) with restricted Access Control List (ACL) communication profiles continues to be a policy requirement for network connected medical devices. An additional enhancement this year to that policy was the requirement that it is a security incident if any network connected medical device is found on the VA network and not isolated in a VLAN with an ACL. As part of the VA's Enterprise Cyber Security Strategy, Medical Cyber Domain, VA will implement a medical device along with additional items over the next year to continue to enhance the safety and security of networked connected medical devices.

Enterprise Change Control Process will be established and will continue ongoing reviews of ACLs against existing rules and guidance documents, Annually Recurring Enterprise networked connected medical device inventory; will be completed. Automated inventory of networked connected devices in medical device VLANs; and Medical Device Vulnerability Management Process will be completed. For Non-OI&T Managed Networks VA Enterprise Cyber Security Strategy, Medical Cyber Domain establishes the foundation for VA to develop a comprehensive cyber security program that will identify, assess and monitor non-OI&T managed devices on the VA network. VA is creating system security plan addendums that will document system personnel responsibilities and inventory each of the systems IP enabled components for the critical infrastructure systems and tenant networks at VA facilities.

Recommendation 19: We recommended the Assistant Secretary for Information and Technology consolidate the security responsibilities for non-OI&T networks present under a common control for each site and ensure vulnerabilities are remedied in a timely manner. (This is a modified repeat recommendation from last year.)

OIT Response: Concur. VA will implement procedures to address security responsibility for network connected devices and for assurance of the timely remediation of vulnerabilities. These procedures will ensure that appropriate security responsibilities for network connected assets are properly assigned under a single authority, inventories of devices are obtained and security assessments are completed. The inventory and assessment documentation will be added to the governance risk and compliance tool, where Information Security Officers will validate compliance with VA policy.

Recommendation 20: We recommended the Assistant Secretary for Information and Technology implement procedures to enforce a standardized system development and change control framework that integrates information security throughout the life cycle of each system. (This is a repeat recommendation from last year.)

OIT Response: Concur. Significant effort has been made to incorporate standardized system development and change management principles across the enterprise and to instill a culture whereby ad hoc and out of band system changes, even if intended to enhance customer experience, are not permitted. Specifically, VA OI&T staff will be required to complete the Change Management training and recorded their result in VA Talent Management System (TMS) for 2016.

In addition to submitting the SDE Standard Operating Procedure (SOP) on configuration management, a bi-annual review of the organizational level Change Management Processes has been implemented in order to identify risks and/or deficiencies personnel not complying to approved policies and procedures. Finally, alignment for configuration management oversight and accountability for the Enterprise is to be assigned to the Enterprise Program Management Office.

Recommendation 21: We recommended the Assistant Secretary for Information and Technology implement processes to ensure information system contingency plans are updated with the required information. (This is a repeat recommendation from last year.)

OIT Response: Concur. VA has implemented annual processes to ensure information system contingency plans are updated with the required information. Additional steps will be taken to ensure system owners are properly reviewing and updating their plans as required. Updates to VA information systems security contingency plans are influenced by several ongoing initiatives: the development of a comprehensive systems inventory as part of the FY 2015 enterprise cybersecurity strategy, the identification of high value assets (HVA) in response to the Federal CIO's July 2015, Cyber Sprint Memorandum, current coordination with the Office of Operations, Security and Preparedness (OSP) to correlate the HVA inventory with those information systems identified as part of their Business Impact Analysis (BIA) reassessment, and the FY 2015 MyVA Regional re-alignment which affected several system accreditation boundaries. The net result will fully align OI&T VA information systems contingency plans with its VA business partners.

The requirement to update and test system contingency plans is an annual event and is outlined in VA Handbook 6500.8, Information system Contingency Planning. Each year, OI&T Information Security (OIS) provides guidance in the form of an action item that provides milestones, templates and actions that need to be completed. During the course of this action, training is provided to Division Chiefs as well as System Owners (or designee). Draft plans are reviewed by Regional Division Chiefs for operational feasibility and OIS Mentors provide feedback as to whether plans are compliant with VA and National Institutes of Standards and Technology (NIST) guidance. After contingency plans are reviewed and approved (pending any necessary changes) by OIS, the system owner signs the plan and uploads to the Governance Risk and Compliance tool.

Recommendation 22: We recommended the Assistant Secretary for Information and Technology develop and implement a process for ensuring the encryption of backup data prior to transferring the data offsite for storage. (This is a repeat recommendation from prior years.)

OIT Response: Concur. In the first phase of a multi-phased process, VA purchased the hardware and software necessary to encrypt backup tapes for our most mission critical system, VistA. The installation of

VistA system backup encryption was completed December 30, 2014. The encryption of VistA data was prioritized ahead of other network storage because it is typically transported to off-site storage facilities and contains our most sensitive patient data. Planning for the next phase of encrypting mission critical systems is currently underway. In this phase, the backups of office automation data copied from disk-to-disk will be encrypted as appropriate and saved on network attached storage systems in secure locations. The plan to ensure encryption of backup data at rest is anticipated to be completed by the end of FY 2016.

Recommendation 23: We recommended the Assistant Secretary for Information and Technology implement improved processes for the testing of contingency plans and failover capabilities for major applications and general support systems to ensure that critical components can be recovered at an alternate site in the event of a system failure or disaster. (This is a new recommendation.)

OIT Response: Concur. VA has implemented annual processes to ensure information system contingency plans are updated with the required information. The Office of Business Continuity within OI&T's, Information Security (OIS) will take additional steps to ensure system owners are properly reviewing and updating their plans as required. Updates to VA information systems security contingency plans are influenced by several ongoing initiatives: the development of a comprehensive systems inventory as part of the FY 2015 enterprise cybersecurity strategy, the identification of high value assets (HVA) in response to the Federal CIO's July 2015, Cyber Sprint Memorandum, current coordination with the Office of Operations, Security and Preparedness (OSP) to correlate the HVA inventory with those information systems identified as part of their Business Impact Analysis (BIA) reassessment, and the MyVA Regional re-alignment which affected several system accreditation boundaries. The net result will fully align OI&T VA information systems contingency plans with its VA business partners.

The requirement to update and test system contingency plans is an annual event and is outlined in VA Handbook 6500.8, Information System Contingency Planning. Each year, OIS provides guidance in the form of an action item that provides milestones, templates and actions that need to be completed. During the course of this action, training is provided to Division Chiefs as well as System Owners (or designee). Draft plans are reviewed by Regional Division Chiefs for operational feasibility and OIS Mentors provide feedback as to whether plans are compliant with VA and National Institutes of Standards and Technology (NIST) guidance. After contingency plans are reviewed and approved (pending any necessary changes) by OIS, the system owner tests the contingency plan, modify or updates as necessary, signs the plan attesting to the accuracy of the plan and uploads to the Governance Risk and Compliance tool.

Recommendation 24: We recommended the Assistant Secretary for Information and Technology perform and document a Business Impact Analysis for all systems and incorporate the results into an overall strategy development effort for contingency planning. (This is a new recommendation.)

OIT Response: Concur. VA recommends that this OIG recommendation be closed. Austin Information Technology Center (AITC) completed a Business Impact Analysis (BIA) for the Financial Management System (FMS), Personnel and Accounting Integrated Data (PAID) System, and VETSNET in November 2015. Copies of the BIA's (embedded below) were submitted to the Enterprise Operations, Risk Management group on December 10, 2015. The BIA results will be included in the existing Information Systems Contingency Plans (ISCP) for these three applications by February 15, 2016. A BIA worksheet to assist the system owner in completion of the BIA is in process. VA Handbook 6500.8, *Information System Contingency Planning,* requires completion of the BIA as a component of the ISCP. Enterprise Operations has a BIA for its customers and will incorporate it into the ISCP process as table tops or functional exercises are conducted.

Recommendation 25: We recommended the Assistant Secretary for Information and Technology implement more effective agency-wide incident response procedures to ensure timely resolution of computer security incidents in accordance with VA set standards. (This is a repeat recommendation from prior years.)

OIT Response: Concur. VA recommends that this OIG recommendation be closed. This is supported by the following: VA Network Security Operations Center (NSOC) initiated a Cyber Incident Response Working Group (IRWG) in March 2014, to improve the VA's Incident Response capability. The Work Group consists of analysts and engineers across the NSOC. The goal of the IRWG is to review current cyber security incident response policies, procedures, and performance measures. The work group provided recommendations which resulted in process updates and an Executive Decision Memo dated March 24, 2014, mandating field personnel adhere to established VA NSOC remediation guidance. Additionally, the IRWG established a reoccurring conference call between the VA NSOC, Field Security Services, and Service Delivery and Engineering to facilitate situational awareness on open tickets and their remediation progress.

The VA NSOC also established monthly metrics to track the effectiveness of the incident response capability and reporting to the US CERT via the Monthly Performance Review. In September 2015, the IRWG updated the VA NSOC Incident Response Plan to include identified incidents are remediated in a timely manner and a FISMA requirement to track enterprise wide metrics for Incident Response. Over the last fiscal year, time to remediate incident ticket has been reduced from 22 days to 1 day on average. OIG noted that VA had implemented a set of metrics and monitoring procedures to assist with incident response. The new monitoring allowed VA to affect a significant downward trend in ticket closure as the year progressed, which covered the last four months of FY 2015.

Recommendation 26: We recommended the Assistant Secretary for Information and Technology identify all external network interconnections and implement improved processes for monitoring all VA internal networks, systems, and exchanges for unauthorized activity. (This is a repeat recommendation from last year.)

OIT Response: Concur. VA will conduct an inventory of VA sites to identify external connections. Validation of each identified connection will occur and those that are found to be non-compliant will enter into a transition to be migrated to the VA Trusted Internet Connection Gateways and decommissioned thereafter. Non-compliant connections will be brought under the control of Network Security Operations Center (NSOC) Security Configuration Services (SCS) with the deployment of an Intrusion Prevention System (IPS) to the site(s) and placed inline.

All contractor hosting facilities connections are now monitored by the VA NSOC Compliance Scanning Services (CSS) Team provides continuous monitoring requirements for VA systems hosted outside the VA network with the use the internal Tenable Security Center Console method to communicate with remote scanners established inside business partner networks. This vulnerability scanning will be expanded to any new remote Business Partner and their remote IP will be a function of the business partner's network and unknown to the CSS team until the remote scanner is configured. VA Directive and Handbook 6513, Secure External Connections, governing the process for managing and continuously monitoring VA connections is in final review.

Recommendation 27: We recommended the Assistant Secretary for Information and Technology implement improved safeguards to prevent data exfiltration from VA networks. (This is a new recommendation.)

OIT Response: Concur. In 2015, the VA began implementing additional features to further protect the VA against exfiltration of data. In addition, we are continuing to research and look at longer term solutions to further protect veteran information. Email security appliances have improved the ability to identify Social Security Numbers within unencrypted email. This has significantly improved the capabilities to include matching patterns that were not identified in earlier versions/technologies. Specific outbound protocols have been limited through. Whitelisting exceptions are documented via Risk-Based Decision (RBD). This is an on-going effort for those exceptions. Secure Socket Layer (SSL) enhanced the VA can inspect fic for specific sites has been piloted. The pilot began in spring 2015 and is on-going. This will be put into production and expanded upon receipt of new Application Firewall Solution to be procured in FY 2016.

Recommendation 28: We recommended the Assistant Secretary for Information and Technology fully develop a comprehensive list of approved and unapproved software and implement continuous monitoring processes to identify and prevent the use of unauthorized software on agency devices. (This is a repeat recommendation from prior years.)

OIT Response: Concur. On a monthly basis VA is identifying unapproved software and blacklisting it from the network. This process began in March 2015, with over 57,000 software applications residing on VA's network. VA is using the Technical Reference Model (TRM) for adjudication and listing of approved software. VA is also teaming with the Department of Homeland Security to implement continuous monitoring capabilities.

Recommendation 29: We recommended the Assistant Secretary for Information and Technology develop a comprehensive software inventory process to identify major and minor software applications used to support VA programs and operations. (This is a repeat recommendation from prior years.)

OIT Response: Concur. In FY 2014, VA OI&T, Architecture, Strategy and Design (ASD) developed and deployed the VA Systems Inventory (VASI) to be the authoritative source of information on VA software applications. VASI provides a comprehensive repository of basic information about over 700 VA systems - both major and minor applications. VA policy, including VA Directive 6500.3, Assessment, Authorization and Continuous Monitoring of VA Information Systems, defines major and minor applications, consistent with NIST 800-18 "Development of System Security Plans," and OMB Circular A-130, Appendix III.

The VASI repository identifies the business function, sponsoring organization, funding information, key stakeholders, geographic location, level of criticality, interfaces with other VA systems, security classification, and technology platforms (e.g. operating system, database management system) for each VA system. The security section of VASI is mapped to RiskVision. VASI has been broadly accepted and integrated into existing governance processes (e.g. Project Management Accountability System) to ensure information is kept current and accurate. The VA utilizes supporting processes such as the RiskVision Working Group, which meets weekly, to review the system inventory including contractor managed systems and also votes to add, update, or decommission FISMA systems within RiskVision.

ASD Office of Technology Strategies maintains the Technical Reference Model (TRM) to provide a whitelist of software technologies and standards approved for use for use to develop, operate, host, and maintain VA applications. The TRM database also contains a blacklist of prohibited technologies. Entries on this list have undergone a strategic assessment based upon the nature of the technology. The TRM database contains guidance, along with any known applicable constraints, on the permissible range of technologies or standards that a VA user, OI&T administration support team or Project Development Team may select or use. The TRM is not intended to direct procurements, although each entry contains available VA licensing information, if known. Requests for an assessment of a technology or standard can be submitted through the TRM tool and will be assessed by subject matter experts (SME's) of the TRM Management Group. Technologies must be operated and maintained in accordance with Federal and Department security and privacy policies and guidelines. Technologies or technical standards that are not listed on the Technology/Standard List are considered unapproved for use. Technologies and technical standards that do not appear on the TRM have not been assessed; either an assessment or a waiver signed by the Deputy CIO of ASD based upon a recommendation from the Architecture and Engineering Review Board, must be obtained in order to use the technology.

Recommendation 30: We recommended the Assistant Secretary for Information and Technology implement procedures for overseeing contractor-managed cloud-based systems and ensuring information security controls adequately protect VA sensitive systems and data. (This is a repeat recommendation from last year.)

OIT Response: Concur. As part of its strategic direction and in accordance with Office of Management and Budget (OMB) direction, VA is looking to more widely deploy cloud-based information technology (IT) solutions to support and enhance the Department's mission. In support of this task, the VA developed a Cloud Strategy to support it pursuance of cloud-based implementations. In conjunction with this effort,

the VA drafted the Cloud Computing Security Handbook consistent with FEDRAMP requirements. This Handbook provides VA policy and roles and responsibilities for cloud computing deployments to address requirements for procedures for overseeing contractor-managed cloud-based systems and the implementation of information security controls in the cloud so that sensitive systems and data are protected. Further, the VA is actively developing the means to better define, develop, and implement of VA cloud security approaches that will maintain the confidentiality, integrity, and availability of Veteran and VA information deployed to cloud solutions. These efforts will ensure VA security policy and guidance documents and other security process are aligned with the overarching cloud strategy and support the cloud execution strategy.

The VA is in the process of finalizing the appointment of the Department's Cloud Broker, the entity who will assume responsibility for cloud-based efforts across the Department. In support of this task, the VA is examining existing roles and responsibilities to implement changes to these roles and further clarify these functions in an effort to ensure cloud mandates are fulfilled. In addition, the VA is actively defining its cyber architecture, an effort that will support cloud architecture decision-making as part of an integrated enterprise architecture strategy.

Recommendation 31: We recommended the Assistant Secretary for Information and Technology implement mechanisms for updating the Federal Information Security Modernization Act systems inventory, including

contractor-managed systems and interfaces, and annually review the systems inventory for accuracy. (This is a repeat recommendation from last year.)

OIT Response: Concur. VA developed a singular repository for FISMA systems located throughout the Department. In addition, the VA utilizes supporting processes such as the Risk Vision Working Group, who meets weekly, to review the system inventory including contractor managed systems and also votes to add, update, or decommission FISMA systems. Further, the VA implemented processes to synchronize the FISMA system list with the systems captured in the VA Systems Inventory (VASI), which is the authoritative source of VA systems. This alignment helps supplement VA's overall management of its FISMA systems inventory.

To improve the accuracy of its Federal Information Security Modernization Act (FISMA) inventory of systems, VA is reviewing its mechanisms for updating the FISMA systems inventory, including contractor-managed systems and interfaces, to include the current annual reviews of the systems inventory for accuracy. VA is also developing updated guidance related to security requirements for the accounting of the inventory of minor systems and low risk impact systems that may be included in the accreditation boundaries for major systems or for general support systems. VA will also update the guidance for the annual inventory of contractor systems to specifically include accounting for system interfaces and interconnection agreements.

Recommendation 2006-03: We recommended the Assistant Secretary for Information and Technology update all applicable position descriptions to better describe position sensitivity levels, and improve documentation of personnel records of "Rules of Behavior" and annual privacy training certifications.

OIT Response: Concur. To ensure position descriptions better describe sensitivity levels and improve documentation of "Rules of Behavior" and annual privacy training certifications, VA requires the use of the Office of Personnel Management's Position Designation System and Automated Tool (PDAT). The VA Office of Human Resources Management (OHRM) issued a generalized Human Resources Management Letter (HRML 05-14-02, dated April 14, 2014) to VA Supervisors reiterating the requirement for using the PDAT, updating PAID, monthly monitoring of P222 report (a Position Sensitivity Report, which allows stations to review the security data for each of their employees on a monthly basis), and a new requirement for annual facility certification that data related to sensitivity level and background investigation and reinvestigation are complete and accurate. The VA Human Resources Information Service (HRIS) also issued two Bulletins (dated April 14, 2014 and Oct 22, 2014) to VA HR leadership regarding the ongoing and new requirements.

Recommendation 2006-04: We recommended the Assistant Secretary for Information and Technology ensure appropriate levels of background investigations be completed for all personnel in a timely manner, implement processes to monitor and ensure timely reinvestigations on all applicable employees and contractors, and monitor the status of the requested investigations.

OIT Response: Concur. Within the Office of Operations, Security and Preparedness (OSP), the Personnel Security & Suitability Program Management Office is in the process of implementing a VA-wide VA Central Adjudication and Background Investigation System (VA-CABS), integrated with Identity, Credential, and Access Management (ICAM) Onboarding solution, which will establish appropriate business rules based on the position description and the sensitivity to conduct investigations and re-investigations. VA-CABS will also monitor investigations and at the 4.5 year mark, a system generated message will be sent to the appropriate security personnel to initiate the re-investigation process. This will minimize the number of individuals with outdated investigations.

OSP has formed the ICAM Program Management Office (PMO) at the direction of the Deputy Secretary of VA. The ICAM mission is to establish an enterprise-wide standardized, integrated, and automated process for onboarding, monitoring, and off-boarding VA Employees, Contractors, Trainees, and Affiliates by establishing authoritative sources of information and unique user identification. Future versions of the system will provide a portal by which VA Volunteers and other affiliates information can be entered directly into the centralized ICAM Onboarding solution.

Recommendation 2006-08: We recommended the Assistant Secretary for Information and Technology reduce wireless security vulnerabilities by ensuring sites have up-to-date mechanisms to protect against interception of wireless signals and unauthorized access to the network, and ensure the wireless network is segmented from the general network.

OIT Response: Concur. VA completed the national wireless modernization project as of August 2015, providing up-to-date mechanisms to protect the wireless network and ensures segmentation of the wireless infrastructure. The solution also provides capabilities to monitor devices within the Wireless Local Area Network (WLAN) and includes a WLAN baseline document defining VA's Wireless configuration. VA has established a team of subject matter experts responsible for the governance of the Wireless Program and has established the Wireless Local Area Network (LAN) Operations Council that will be responsible for the operational aspects of the VA wireless LAN and any changes in technologies or improvements.

Also based on what was identified by the work completed on the Plan of Action, VA is also finalizing a review and collection of VA Wireless documentation. VA has developed a wireless detection procedure, and developed a training curriculum for WLAN for those involved in WLAN implementation and Maintenance.

Recommendation 2006-09: We recommended the Assistant Secretary for Information and Technology identify and deploy solutions to encrypt sensitive data and resolve clear text protocol vulnerabilities.

OIT Response: Concur. VA has completed the implementation of encryption for sensitive data in transit on major data circuits connecting medical centers and data centers throughout the enterprise and continues to implement encryption on remaining data circuits and router upgrades.

Appendix E OIG Contact and Staff Acknowledgements

OIG Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Acknowledgments	Michael Bowman, Director Carol Buzolich Jerry Charles Richard Purifoy Juan Rivera Felita Traynham Richard Wright

Appendix F 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 report is available on our Web site at www.va.gov/oig.