VA Office of Inspector General

OFFICE OF AUDITS & EVALUATIONS

Department of Veterans Affairs

Federal Information Security Management Act Audit for Fiscal Year 2014

May 19, 2015
14-01820-355

ACRONYMS

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
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plans of Action and Milestones
VA	Department of Veterans Affairs

DEPARTMENT OF VETERAN AFFAIRS

Memorandum

Date: May 05, 2015

From: Assistant Inspector General for Audits and Evaluations

Subj: VA's Federal Information Security Management Act Audit for Fiscal Year 2014

To: Executive in Charge for Information and Technology

1. Enclosed is the final audit report, *Federal Information Security Management Act Audit for Fiscal Year 2014*. The 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 Management 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 due to the nature and maturity of its information security program. In order to better achieve FISMA outcomes, VA needs to focus on several key areas including:

   - Addressing security-related issues that contributed to the information technology material weakness reported in the fiscal year (FY) 2014 audit of VA's consolidated financial statements
   - Successfully remediating 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. The OIG does not express an opinion on the effectiveness of VA's internal controls during FY 2014. Our independent auditors will follow up on the outstanding recommendations and evaluate the adequacy of corrective actions during their FY 2015 FISMA audit.

5. This report provides 33 recommendations for improving VA's information security program; 27 recommendations are included in the report body and 6 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 FY 2014 FISMA audit. VA successfully closed five recommendations and we identified three new recommendations in FY 2014.
6. The effect of these open recommendations will be considered in the FY 2015 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.

LINDA A. HALLIDAY
Assistant Inspector General
for Audits and Evaluations

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

April 20, 2015

The Honorable Richard Griffin
Acting Inspector General
Department of Veterans Affairs
801 I Street, Northwest
Washington, DC 20001

Dear Mr. Griffin:

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, 2014 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.

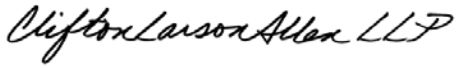
We have performed the FISMA performance audit, using procedures prepared by CliftonLarsonAllen LLP and approved by the Office of the Inspector General (OIG), during the period April 2014 through November 2014. Had other procedures been performed, or other systems subjected to testing, different findings, 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 2014. 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



GFF:sgd

Report Highlights: Federal Information Security Management Act Audit for Fiscal Year 2014

Why We Did This Audit

The Federal Information Security Management Act (FISMA) requires agency Inspectors General to annually assess the effectiveness of agency information security programs and practices. Our fiscal year 2014 audit determined 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 has made progress developing policies and procedures but still faces challenges implementing components of its agency-wide information security 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 standards on all servers, databases, and network devices. VA also has not effectively implemented procedures to identify and remediate system security vulnerabilities on network devices, database, and server platforms VA-wide.

Further, VA has not remediated approximately 9,000 outstanding system security risks in its corresponding Plans of Action and Milestones to improve its information security posture. As a result, the fiscal year 2014 consolidated financial statement audit concluded that a material weakness still exists in VA's information security program.

What We Recommended

We recommended the Executive in Charge for Information and Technology implement comprehensive measures to mitigate security vulnerabilities affecting VA's mission-critical systems.

Agency Comments

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

LINDA A. HALLIDAY
Assistant Inspector General
for Audits and Evaluations

Table of Contents

Introduction 1

Results and Recommendations 2

Finding 1 Agency-Wide Risk Management Program 2

Finding 2 Identity Management and Access Controls 7

Finding 3 Configuration Management Controls 10

Finding 4 System Development/Change Management Controls 13

Finding 5 Contingency Planning 14

Finding 6 Incident Response and Monitoring 15

Finding 7 Continuous Monitoring 17

Finding 8 Contractor Systems Oversight 19

Finding 9 Security Awareness Training 20

Appendix A Status of Prior-Year Recommendations 22

Appendix B Background 26

Appendix C Scope and Methodology 28

Appendix D Executive in Charge for Information and Technology Comments 30

Appendix E Office of Inspector General Contact and Staff Acknowledgements 56

Appendix F Report Distribution 57

INTRODUCTION

Objective

The objective of this audit was to determine the extent to which VA's information security program and practices comply with Federal Information Security Management 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) 2014 FISMA audit.

Overview

Information security is a high-risk area Government-wide. Congress passed the E-Government Act of 2002 (Public Law 107-347) 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 65 major applications and general support systems at 23 VA facilities. In FY 2014, the teams identified specific deficiencies in the following areas.

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

This report provides 33 total recommendations, including 3 new recommendations, for improving VA's information security program. Twenty-seven recommendations are included in the report body and six recommendations are provided in Appendix A. The appendix addresses the status of prior recommendations not included in the report body and VA's plans for corrective action. The FY 2013 FISMA report provided 35 recommendations for improvement.

RESULTS AND RECOMMENDATIONS

Finding 1 Agency-Wide Risk Management Program

FISMA requires each Federal agency to develop, document, and implement an agency-wide information security risk management program. VA has made progress developing 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 Remain

In 2007, VA issued VA Directive 6500, *Information Security Program,* and VA Handbook 6500, *Information Security Program*, defining the high-level policies and procedures to support its agency-wide information security risk management program. In FY 2012, VA updated VA Handbook 6500 to be consistent with revised NIST Special Publications and to supplement existing VA directives and handbooks. OMB Memorandum M-15-01, *FY 2014-2015 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management Practices,* issued in October 2014, 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 2014 related to:

- Training, both role-based and security awareness
- Testing contingency plans
- Reducing the number of individuals with outdated background investigations

- Implementing predictive scanning that allows for the identification of vulnerabilities across field offices
- Implementing an IT governance, risk, and compliance tool to improve processes for assessing, authorizing, and monitoring the security posture of VA systems
- Ensuring consistent compliance with U.S. Government Configuration Baseline standards

However, these controls require 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. While VA has implemented the new RiskVision Governance Risk and Compliance (GRC) tool for the purpose of enterprise wide risk and security management, this FISMA audit identified deficiencies related to VA's overall risk management approach, Plans of Action and Milestones, and system security plans, which are discussed in the following sections. Each of these processes is critical 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 framework; however, security risks were not fully communicated to the data centers, regional offices, and medical facilities that we visited. Additionally, VA has not ensured that its information security controls were effectively monitored on an ongoing basis and adequately documented, and system assessments and authorizations were not performed in accordance with Federal standards.

For example, VA prematurely issued Temporary Authorization to Operate for the Regions, Enterprise Operations Service Lines, and major applications. These temporary authorizations were issued prior to the completion of security assessment and authorization activities as required by NIST Special Publication 800-37 Rev 1. Moreover, OMB does not recognize an Interim (temporary) Authority to Operate systems. We also noted certain deficiencies with the temporary system authorizations such as ensuring that all security documentation was completed or security configuration and penetration testing was performed by proposed deadlines. Subsequently, systems were provided additional extensions resulting from the lack of compliance with previous authorization packages.

Further, risk assessments did not consider all known system security risks such as unresolved Plan of Action and Milestones, unsecure tenant systems, unprotected medical devices, and vulnerability scans results. Moreover, the business effect and recommended corrective actions for risk assessment results were not identified for all risks. 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 is still ongoing and enterprise-wide risks have not been fully identified or mitigated with appropriate risk mitigation strategies.

Plans of Action and Milestones

OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones* (POA&M), 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 9,000 open POA&Ms in FY 2014 as compared with 6,000 open corrective actions in FY 2013. POA&Ms identify which actions must be taken to remediate system security risks and improve VA's overall information security posture. VA did not initially include legacy POA&Ms within the GRC tool when the system implementation launched in early FY 2014. In, April 2014, VA began to migrate legacy POA&Ms into the GRC tool in response to our finding.

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, many POA&Ms were closed based upon Executive Decision Memoranda or Risk-Based Decision Memoranda. However, system security risks still remain as the underlying weaknesses were not fully remediated.

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 remediate 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. Further, 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. Many of these documentation issues were related to the GRC tool's limited functionality for generating comprehensive system security plans and other documents. Additionally, VA did not provide sufficient training regarding the use of the GRC tool prior to implementation.

VA Handbook 6500, Appendix F provides guidelines on maintaining and updating system security plans for major applications and general support systems. However, VA Security Handbook 6500 was not updated to reflect current Federal standards as stated in NIST Special Publication 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations.* 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 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.)*

2. We recommended the Executive in Charge 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 modified repeat recommendation from last year.)*

3. We recommended the Executive in Charge for Information and Technology implement clear roles, responsibilities, and

accountability for developing, maintaining, completing, and reporting Plans of Action and Milestones. *(This is a modified repeat recommendation from prior years.)*

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

6. We recommended the Executive in Charge for Information and Technology implement improved processes for 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 modified 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 the following 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 remediated 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. In August 2014, we reported that certain audit controls within VistA were not enabled, which limited our ability to determine whether any malicious manipulation of the VistA data occurred at the Phoenix VA Medical Center.[1] Moreover, we have identified and reported deficiencies with audit logging for more than 8 years in our annual FISMA reports.

Remote Access

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

7. We recommended the Executive in Charge for Information and Technology implement mechanisms to enforce VA password policies and standards on all operating systems, databases,

[1] *Review of Alleged Patient Deaths, Patient Wait Times, and Scheduling Practices at the Phoenix VA Health Care System* (Report No. 14-02603-267, August 26, 2014)

applications, and network devices. *(This is a repeat recommendation from prior years.)*

8. We recommended the Executive in Charge 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.)*

9. We recommended the Executive in Charge 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.)*

10. We recommended the Executive in Charge for Information and Technology implement two-factor authentication for remote access throughout the agency. *(This is a repeat recommendation from prior years.)*

11. We recommended the Executive in Charge 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 identify 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 should 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 remediate 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 remediate security weaknesses on databases hosting mission-critical applications. Unsecure database configuration settings can 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 remediate 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 remediate 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. In response to our findings, in July 2014, VA established a Medical Device Protection Program Leadership Workgroup to address these issues and implement corrective actions.

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. These organizations or "tenant networks" had significant critical or high-risk vulnerabilities that weaken the overall security posture of the local sites. 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 85 to 94 percent, with United States Government Configuration Baseline standards for end-user systems. More specifically, we identified seven VA facilities with compliance ratings under 90 percent when compared to

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. 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

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

13. We recommended the Executive in Charge 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 modified repeat recommendation from last year.)*

14. We recommended the Executive in Charge for Information and Technology implement improved processes for monitoring standard security configuration baselines for all VA operating systems, databases, applications, and network devices. (*This is a modified repeat recommendation from last year.)*

15. We recommended the Executive in Charge for Information and Technology implement improved network access controls to ensure medical devices and tenant networks are appropriately segregated from general networks and mission-critical systems. (*This is a new recommendation)*

16. We recommended the Executive in Charge for Information and Technology consolidate the security responsibilities for tenant networks present under a common control for each site and ensure vulnerabilities are remediated in a timely manner. *(This is a new recommendation)*

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 identify software changes to mission-critical systems and infrastructure network devices that did not follow standardized software change control procedures.

FISMA Section 3544 requires establishing 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 identified numerous test plans, test results, and approvals that were either incomplete or missing. Specifically, at one major data center and four VA Medical Centers, we noted that change management policy and procedures for authorizing, testing, and approving system changes was not 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

17. We recommended the Executive in Charge 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 modified repeat recommendation from last year.)*

Finding 5 Contingency Planning

Overall, we noted a continued improvement in contingency plan testing since our FY 2012 audit. However, VA contingency plans still were not fully documented or reflecting current environments. VA Handbook 6500, Appendix F establishes high-level policy and procedures for contingency planning and plan testing. Our audit identified the following deficiencies related to contingency planning.

- 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 lessons learned from testing contingency plans at alternate processing and storage sites. We identified this issue at five VA Medical Centers and a contractor facility.
- Backup tapes for mission-critical systems were not encrypted prior to transporting data offsite for storage. We identified this issue at two major data centers and seven VA Medical Centers. VA has identified the lack of backup tape encryption as a vulnerability and has developed a corrective action plan to encrypt backup tapes during FY 2015.

Incomplete documentation of contingency and disaster recovery plans may prevent 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

18. We recommended the Executive in Charge for Information and Technology implement processes to ensure information system contingency plans are updated with the required information. *(This is a modified repeat recommendation from last year.)*

19. We recommended the Executive in Charge 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.)*

Finding 6 Incident Response and Monitoring

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 prevented VA's Network and Security Operations Center from periodically testing certain systems for security vulnerabilities. Consequently, the Network and Security Operations Center does 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 prevent VA from detecting and responding to intrusion attempts in a timely manner.

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. Despite Federal requirements, we performed seven unannounced scans of internal networks; however, only three vulnerability scans were detected by intrusion detections sensors and only one of those scans was ultimately blocked by VA. Audit teams also identified other deficiencies related to VA's security incident management and network monitoring processes that are discussed below.

VA performs significant monitoring of its known Internet gateways to identify and respond to computer security events and potential network intrusions. This monitoring includes some event correlation, which ties multiple entries together to identify larger trends, intrusions, or intrusion attempts. However, VA is not capturing incident response reporting metrics in accordance with its Incident Response Plan. For example the plan requires capturing various security event metrics such as "Mean Time to Identify" and "Mean Time to Verify." Nevertheless, VA has not captured these metrics but plans on monitoring these areas within the next fiscal year. To improve incident management, VA continues to implement its Trusted Internet Connection initiative to identify all system interconnections and consolidate them into four VA gateways. Although progress has been made in cataloging the many interconnections for monitoring purposes, unmonitored connections still exist. Ineffective monitoring of external network interconnections could prevent VA from detecting and responding to intrusion attempts in a timely manner. Furthermore, VA's enterprise risk management cannot be fully effective without comprehensive monitoring all external network connections.

Our audit continued to identify numerous high-risk computer security incidents, including malware infections, that were not remediated in a timely manner. Specifically, we noted a high number of malware security incident

tickets that took more than 30 days to remediate and close. We also noted numerous Kuluoz infections[2] that remain unresolved for significant periods of time. While VA's performance has improved from the prior year, the process for tracking higher-risk tickets remained inefficient, and some computer security incidents were not remediated. By contrast, NIST Special Publication 800-61, *Computer Security Incident Handling Guide,* provides examples of computer security incident response times ranging from 15 minutes to 4 hours, based on 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.

Recommendations

20. We recommended the Executive in Charge 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.)*

21. We recommended the Executive in Charge for Information and Technology identify all external network interconnections and implement improved processes for monitoring VA networks, systems, and exchanges for unauthorized activity. *(This is a modified repeat recommendation from last year.)*

22. We recommended the Executive in Charge for Information and Technology implement and monitor incident response metrics to assist in tracking and remediating all cybersecurity events. (*This is a new recommendation*)

[2] Kuluoz trojans attempt to steal user passwords, sensitive information, and can be used to download other malware onto infected computers.

Finding 7 Continuous Monitoring

VA lacks an effective continuous monitoring program to identify unsecure system configurations or monitoring for unauthorized software and hardware devices. In addition, VA has not implemented effective processes for removing unauthorized software on its systems. Moreover, VA has not fully developed a software inventory to identify 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.

Because of inadequate VA monitoring procedures, our technical testing 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 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. Without effectively monitoring software and applications installed on VA devices, malicious users may 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 that supports operational security demands for protection of critical information. This framework is 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 continues to develop and implement Continuous Monitoring processes to better protect VA systems. The goal of *Information Security Continuous Monitoring* is to examine the enterprise to develop a real-time analysis of actionable risks that may adversely affect mission-critical systems.

VA has 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. Further, VA has deployed various software and configuration monitoring tools to VA facilities as part of its "Visibility to Server" and "Visibility to Desktop" initiatives. However, VA has 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. Additionally, 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

23. We recommended the Executive in Charge for Information and Technology develop a listing of approved software and implement continuous monitoring processes to identify and prevent the use of unauthorized application software, hardware, and system configurations on its networks. *(This is a repeat recommendation from prior years.)*

24. We recommended the Executive in Charge 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 2014, 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 establishment of security requirements for all VA contracts involving sensitive VA information. Despite these requirements, our audit disclosed several deficiencies in VA's contractor oversight activities in FY 2014. 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 does 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 cannot ensure that contractor security controls adequately protect sensitive systems and data in accordance with its information security requirements.

Recommendations

25. We recommended the Executive in Charge 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 modified repeat recommendation from last year.)*
26. We recommended the Executive in Charge for Information and Technology implement mechanisms for updating the Federal Information Security Management Act systems inventory, including contractor-managed systems and interfaces, and annually review the systems inventory for accuracy. *(This is a repeat recommendation from prior years.)*

Finding 9 Security Awareness Training

As part of the CRISP initiative, we noted improvements in providing users with required role-based and security awareness training. However, VA has not fully implemented automated processes to track security awareness training for residents, volunteers, and contractors at all VA facilities. As a result, our testing identified personnel who had not completed VA's security awareness training at some VA facilities. VA Handbook 6500, Appendix D establishes high-level policy and procedures for VA's security awareness training program, requiring all users of sensitive information to annually complete VA's security awareness training.

VA uses the Talent Management System, an online training system, to provide user access to a number of online training resources and track required security awareness and other training for VA employees and contractors. However, VA relies on manual processes to track fulfillment of training requirements for residents, contractors, and volunteers, as automated tracking mechanisms have not been fully implemented. Without automated tracking to support centralized monitoring of user training, management cannot ensure that these personnel complete the annual security awareness training requirements. Computer security awareness training is essential to help employees and contractors understand their information security and privacy responsibilities.

Recommendation

27. We recommended the Executive in Charge for Information and Technology implement mechanisms to ensure all users with VA network access participate in and complete required VA-sponsored security awareness training. *(This is a repeat recommendation from prior years.)*

Summary of Response From the Executive in Charge for Information Technology

The Executive in Charge for Information and Technology concurred with the 33 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. In his comments, the Executive in Charge for Information and Technology stated that VA has made substantial progress in implementing the recommendations from FY 2013 and requests the closure of six recommendations in the FY 2014 report. The Executive in Charge for Information and Technology provided several examples of improved security controls resulting from our past recommendations. We will not close any recommendations until relevant information security policies and procedures are finalized and information security control deficiencies are fully remediated. We will continue to evaluate VA's progress during our audit of VA's information security program in FY 2015. 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. Status of Prior Year Recommendations

Number	Recommendation	Status (In Progress or Closed)	Estimated Completion	Corrective Actions
FY 2013–27	We recommended the Executive in Charge for Information and Technology develop guidance and procedures to integrate information security costs into the capital planning process while ensuring traceability of Plans of Action and Milestones remediation costs to appropriate capital planning budget documents.	In Progress	May 2015	OI&T has developed updated Standard Operating Procedures requiring the inclusion of all Plans of Action and Milestones within VA's Planning, Programming, Budgeting, and Execution process. The revised procedures will provide traceability of project security costs throughout the Capital Planning and Investment Control process. Capital planning exceptions continued to be identified during FY 2014 FISMA testing.

Number	Recommendation	Status (In Progress or Closed)	Estimated Completion	Corrective Actions
FY 2010–21	We recommended the Assistant Secretary for Information and Technology develop mechanisms to ensure risk assessments accurately reflect the current control environment, compensating controls, and the characteristics of the relevant VA facilities.	Requested Closure	To Be Determined	VA has implemented the GRC tool as a major element of implementing an agency-wide risk management governance structure. The tool is capable of tracking the real-time security posture of VA systems and provides the mechanism to identify, monitor, and manage risks across the enterprise. Risk assessment exceptions continued to be identified during FY 2014 FISMA testing.

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 employee/contractor personnel records of "Rules of Behavior" and annual privacy training certifications.	In Progress	November 2016	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 2014, 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 applicable VA employees and contractors 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	November 2016	VA is implementing a 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 investigations continued to be identified during FY 2014 FISMA testing.

Number	Recommendation	Status (In Progress or Closed)	Estimated Completion	Corrective Actions
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	October 2015	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 2014 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	December 2015	VA has launched a project to encrypt sensitive data transmitted over external and internal data circuits and resolve clear text protocol vulnerabilities. Clear text protocol vulnerabilities continued to be identified during our FY 2014 FISMA testing.

Appendix B Background

On December 17, 2002, then-President George W. Bush signed FISMA into law, reauthorizing key sections of the Government Information Security Reform Act. 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. VA's security program should protect the information systems that support operations, including those provided or managed by another agency, contractor, or other source. As specified in FISMA, agency heads are responsible for conducting annual evaluations of information security programs and practices.

FISMA also requires agency Inspectors General to assess the effectiveness of agency information security programs and practices. Guidance has been issued by OMB in both circulars and memos and by NIST in its 800 series of special publications supporting FISMA implementation covering significant aspects of the law. In addition, Federal Information Processing Standards have been 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 2014, OMB issued Memorandum M-15-01, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*. Federal agencies are to focus on implementing the Administration's three cybersecurity priorities: (1) Continuous Monitoring, (2) Trusted Internet Connection capabilities and traffic consolidation, and (3) Strong authentication using Personal Identity Verification cards for logical access. The FY 2014 FISMA metrics issued by DHS established minimum and target levels of performance for these priorities, as well as metrics for other key performance areas. To comply with the reporting requirements, agencies must carry out the following activities.

- Chief Information Officers should submit monthly data through CyberScope, the FISMA reporting application. Agencies must upload data from their automated security management tools into CyberScope on a monthly basis for a specified number of data elements.
- Agencies must respond to security posture questions on a quarterly and annual basis. These questions address areas of risk and are designed to assess the implementation of security capabilities and measure their effectiveness.

- 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 developing a complete inventory of major information systems, providing security training to personnel, testing and evaluating security controls, and testing continuity plans. The OIG contracted with the independent accounting firm CliftonLarsonAllen LLP to conduct the annual FISMA audit for FY 2014. The 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 NIST guidance during its audit. Audit procedures included reviewing policies and procedures, interviewing employees, reviewing and analyzing records, and reviewing supporting documentation. The 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 23 VA facilities to 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 2014 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. Sites selected for testing included:

- Information Technology Center—Austin, TX
- VA Medical Facility—Charleston, SC
- VA Medical Facility—Cheyenne, WY
- Terremark, Cloud Service Provider—Culpepper, VA
- VA Medical Facility—Des Moines, IA
- VA Medical Facility—Fresno, CA
- Information Technology Center—Hines, IL
- VA Medical Facility—Honolulu, HI
- VA Medical Facility—Indianapolis, IN

- VA Medical Facility—Louisville, KY
- Network and Security Operations Center—Martinsburg, WV
- Capitol Regional Readiness Center—Martinsburg, WV
- VA Medical Facility—New York, NY
- VA Regional Office—New York, NY
- Information Technology Center—Philadelphia, PA
- VA Insurance Center—Philadelphia, PA
- VA Medical Facility—Pittsburgh, PA
- VA Regional Office—Pittsburgh, PA
- Loan Guaranty Contractor Managed Facility—Plano, TX
- National Cemetery Administration—Quantico, VA
- VA Medical Facility—Temple, TX
- VA Medical Facility—Wilmington, DE
- 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 Executive in Charge for Information and Technology Comments

Department of Veterans Affairs

Memorandum

Date: April 15, 2015

From: Executive in Charge and Chief Information Officer, Office of Information and Technology (005)

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

To: Assistant Inspector General for Audits and Evaluations

1. VA appreciates the opportunity to respond to the Office Inspector General's (OIG) 2014 Federal Information Security Management Act assessment (FISMA). As the OIG's assessment has noted, VA has made substantial progress in implementing the recommendations from Fiscal Year (FY) 2013. We have continued this progress and as a result are requesting closure for six of the recommendations in the FY 2014 report. However, there is still work to be done and we are committed to continuing our aggressive efforts in protection our veteran's and employee's data. Our efforts will be built upon the progress made in 2013 and 2014; For example:

   - VA has implemented a "documentation support effort" to ensure that FISMA documentation is standardized across the enterprise. This effort also is responsible for the enterprise-wide standardization of conditions for Plans of Action and Milestones closure, progress, roles, and responsibilities. The effort ensures that these conditions are implemented appropriately within VA's Governance, Risk, and Compliance tool (GRC).
   - In addressing findings regarding security accreditation boundaries and Privacy Impact Assessments (PIA), VA will be mindful of impending changes stemming from the *MyVA* reorganization effort. *MyVA* will significantly impact the VA security accreditation boundaries, and as a result, VA will be making changes to these boundaries once *MyVA* plans have been finalized. VA has made significant progress in its security accreditation and PIA processes, and these enhancements activities will continue for the next several years. VA will continue to modify and enhance the FISMA documentation across the enterprise and address any PIAs that will also be affected by *MyVA.*
   - VA has made substantial progress towards addressing the Remote Access recommendations since the end of the FY 2014 FISMA reporting period. VA is pleased that the OIG has recognized this progress and consequently has recommended the closure of several past findings. VA will continue its efforts to strengthen its security posture surrounding Remote Access in order to completely address the remaining open findings.
   - Another area in which VA has made great strides is in the implementation of an enterprise-wide configuration and vulnerability management

program. Prior to this implementation, regional programs were responsible for configuration and vulnerability management. While these regional efforts were effective, they were not consistently implemented across the enterprise. VA's enterprise-wide program ensures that VA's configuration and vulnerability management processes are carried out consistently across the enterprise and that VA's 1.4 million endpoints are being effectively managed.

- In today's environment, VA and the OIG agree that incident response and remediation is as important as network defense. VA is already nationally recognized for its incident response procedures and continues to investigate ways that these procedures can be improved. When responding to an incident of any kind, organizations must be able to incorporate information from a variety of operational pillars. To this point, VA has begun to develop a process in which responses to all types of incidents, including those that are operational, privacy, cyber-related, will be centrally handled, triaged, and executed.

2. The changes we have implemented through 2013 and 2014 have shown positive progress for an additional Thirteen of the enclosed recommendations, but instead of declaring success and requesting closure of these recommendations because all the necessary policy framework and procedures are in place, as we would have done in the past, we are spending this fiscal year performing compliance reviews before requesting closure in October of this year. We are committed to working with our OIG partners to assess the state of VA's FISMA implementation and look forward to our continued partnership to ensure the safety and integrity of Veterans' data.

Stephen W. Warren

Attachment

Attachment

Office of Information and Technology
Comments to Draft OIG Report,
"Federal Information Security Management Act Audit for FY 2014"
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. In March 2015, the Office of Information and Technology (OI&T) issued a new version of VA Handbook 6500, "Risk Management Framework for VA Information Systems - Tier 3: VA Information Security Program," which is based on National Institute for Standards and Technology (NIST) Special Publication 800-53 Revision 4. This revised handbook brings the Department's security policy into full compliance with Federal requirements for an agency-wide risk management framework and governance structure, including requirements for the mechanisms and processes that will better enable the Department to identify, monitor, and manage risks across the VA enterprise. Governance is provided in the "Roles and Responsibilities" section of this handbook.

Recognizing that the introduction of a GRC tool would take some time for the staff to become accustomed to its powerful capabilities, OI&T has continued to make steady progress through 2014 and 2015 in maturing the use of the features of the GRC tool. The GRC tool is now serving as a major element supporting VA's implementation of an agency-wide risk management governance structure. The GRC tool is VA's robust repository capable of tracking the real-time security posture of VA's IT systems and provides the mechanism to identify, monitor, and manage risks across the enterprise. The tool is used in concert with existing IT monitoring and tracking tools, such as IBM End-Point Manager (IEM), Solar Winds, and NESSUS, to extract up to 54 NIST controls in real time, while capturing the remaining controls via automated workflows. The Risk Vision GRC tool automatically ties risk assessments to POA&Ms and system security plans, resulting in a more comprehensive understanding of VA's security posture, far exceeding any past capabilities. The workflow process of entering information into the GRC tool ensures that only the most current risk information is retained. This is also true of the System Security Plan and Federal Information Processing Standards (FIPS) assessments.

Ultimately, the automated workflow processes provide timely risk information, including the results of security controls assessment testing, to all individuals that provide inputs into the system security assessment and authorization process. The CIO is then presented with a comprehensive set of evidence that supports the risk-based determination of Authority to Operate (ATO) decisions. OI&T also maintains a mature Enterprise Risk Management (ERM) organization that proactively manages risks that are applicable to the OI&T enterprise. Within ERM, the Risk Assessment and Mitigation (RAM) office has an IT Security and Compliance Risk Division that is focused on the assessment and mitigation of information security risks that

meet the organization's definition of enterprise-level risk. The Office of Information Security (OIS) also has a Risk Management office that addresses information security risks that do not rise to the level of OI&T enterprise risks.

Target Completion Date: OI&T is recommending that this recommendation be closed - supporting material will be provided under separate cover.

Recommendation 2: We recommended the Executive in Charge 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 modified repeat recommendation from last year.)

OI&T Response: Concur. The GRC tool, implemented at the end of FY 2013, monitors the real-time security posture of the VA's IT systems. This tool is the mechanism used to track active POA&Ms. The GRC tool is also the sole repository for all supporting artifacts that are necessary to support POA&M processes and serves to maintain the sufficient documentation that is needed to justify and support the closure of POA&Ms.

Throughout 2014 and 2015, VA has further matured its use of the GRC tool for POA&M tracking and reporting. The results of security controls assessments and other identified system weaknesses are captured in POA&Ms, which are now being routinely entered into the GRC tool. Progress in closing POA&Ms and the status of open POA&Ms is part of the information that is presented within the work flow processes that support the risk-based determination for a system ATO.

Additionally, mechanisms such as compliance reviews conducted by OCS staff, quarterly self-assessments by facility staff, and control implementation validation by Information Security Officers (ISO) are currently in place to check POA&M documentation. These mechanisms also ensure that documentation is adequate and sufficient to justify closure decisions. The CRISP PMO is also providing oversight to validate that the use of the GRC tool by VA staff will mature to the point that will enable VA to close this recommendation by the end of FY 2015.

Target Completion Date: September 30, 2015

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

OIT Response: Concur. Clearly defined roles and responsibilities for developing, maintaining, completing and reporting POA&Ms are found in VA Handbook 6500 and VA Handbook 6500.3. Section 4 of VA Handbook 6500 includes information security responsibilities regarding POA&Ms for staff members, including: the Deputy CIO for SDE, system owners, the Executive Director for Quality, Performance and Oversight, Under Secretaries, Assistant Secretaries, program directors, facility directors, ISOs, local program management, local CIOs, system administrators, network administrators, database managers, contracting officer representatives,

local HR staff, security and law enforcement staff, and other key officials. POA&M responsibilities are also addressed in VA Handbook 6500 in Appendix F under Controls CA-5: Plan of Action and Milestones and PM-4: Plan of Action and Milestones.

Section 3 of VA Handbook 6500.3 includes roles and responsibilities regarding POA&Ms for the VA CIO, OIS Deputy Assistant Secretary (DAS), system owners, project managers, information/data owners, local CIOs, system administrators, network administrators, and ISOs. Appendix E describes the process for developing the POA&M in the Authorization process. The use of the POA&M features within the GRC Risk Vision tool has continued to mature through 2014 and 2015. The tool is now actively being used to provide an automated method for assigning POA&M management roles and responsibilities to system owners, information security officers, administrators, and managers. The CRISP Program Management Office (PMO) is also providing oversight to validate that the use of the GRC tool by VA staff will mature to the point that will enable VA to close this recommendation by the end of FY 2015.

Target Completion Date: September 30, 2015.

Recommendation 4: We recommend the Executive in Charge 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 last year.)

OIT Response: Concur. The GRC tool, implemented in August 2013, establishes mechanisms to ensure that POA&Ms are updated with current status information. These mechanisms are inherent in the work flow of the tool and provide the necessary checks and balances to ensure that information can be entered accurately. Through 2014 and 2015, VA has continued to refine and mature its use of the powerful features in the GRC tool, including the capabilities to ensure POA&Ms are updated to accurately reflect current status information.

A two-step validation process is integral to the specially designed workflows of RiskVision. The information security control provider is required to provide evidence of the control implementation status. The assigned ISO is required to validate the implementation status. If found to be deficient or inaccurate, the ISO generates a finding. Additionally, with the IEM feeds being collected by RiskVision, automated compliance checks are reported without requiring user intervention. This allows VA to determine the compliance of a device that is part of an accreditation boundary.

The GRC tool is the sole repository of all active POA&Ms and is actively used to manage the POA&M process. To further refine and enhance the consistency and accuracy of the POA&M process, VA is implementing a comprehensive standard operating procedure (SOP) to further augment existing policies and procedures so that POA&M processes are fully utilized across VA. The policies established in the SOP will also ensure that POA&Ms continue to be updated to accurately reflect current status information. The CRISP PMO is also providing oversight to validate that the use of the GRC tool by VA staff will mature to the point that will enable VA to close this recommendation by the end of FY 2015.

Target Completion Date: September 30, 2015.

Recommendation 5: We recommend the Executive in Charge for Information and Technology develop mechanisms to ensure system security plans reflect current operational environments, including accurate system interconnection, boundary and ownership information. (This is a modified repeat recommendation from last year.)

OIT Response: Concur. In concert with the implementation of the GRC tool in August 2013, the accreditation boundaries for all VA systems were evaluated, reassessed and restructured. This ensured that the system security plans inherent in the GRC tool reflected the current operational environments and that system interconnections were assessed for accuracy. The GRC tool provides the mechanisms for VA to ensure the accuracy of system security plans. System security plan documentation is checked for accuracy as one of the major considerations to support the risk-based decision for issuance of an ATO, particularly in the workflows that support the Assessment and Authorization process. The GRC tool also captures current system ownership and can be easily updated. The GRC tool is the sole repository for the system security plans ensuring proper oversight of status updates.

In addition, VA policy requires all system owners to have accurate, comprehensive and up-to-date system security plans which are assessed as part of the accreditation process. Finally, to further ensure that the content within all system security plans is accurate and up to date, VA established a contract in early 2015 that enables the Department to re-validate the accuracy of security plans. All documentation will be reviewed, assessed, and updated as needed, for all information systems accredited by VA. As VA re-aligns its organizational structure, it will continue to be an ongoing requirement for the Department to update its security plans to properly reflect updated operational environments, including any changes to system interconnections, boundary, and ownership information.

In late 2014, updates were implemented within the headquarters instance of the GRC tool to enable security documentation to include the NIST 800-53 Rev 4 security controls. The tool will be further enhanced in 2015 to also address the capability to include NIST 800-53 Rev 4 privacy controls in all system security plans, privacy impact assessments, and security controls assessments. VA is developing a transition plan to move all VA systems currently maintained in the GRC instance at the Austin Information Technology Center (AITC) to the headquarters instance of the GRC. This will enable the VA to have a single GRC system for all VA systems. The effort to have the headquarters instance of the GRC tool updated with capabilities to fully address NIST 800-53 Rev 4 security and privacy controls for all system security and privacy documentation will be completed in the summer of 2015.

Target Completion Date: September 30, 2015

Recommendation 6: We recommend the Executive in Charge for Information and Technology implement improved processes for 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 modified repeat recommendation.)

OIT Response: Concur. With the implementation of the GRC tool in August 2013, a new and improved process was developed and established for all IT system security risk assessments and other security documentation. Based on actual findings, which flows through the automated system, we are now annually and continuously monitoring and managing risk assessments. This process enables us the ability to compare and contrast data, leading to improved security impact analyses. We are also able to proactively introduce process and policy changes, based upon analysis of information discovered in the security assessment phase.

The automated manner in which this is now managed has greatly improved the process used for updating all security documents, as updates are accomplished throughout the year. Analysis of the data ensures that remediation activities are appropriate to the current environment. In late 2014, updates were implemented within the headquarters instance of the GRC tool to enable security documentation to include the NIST 800-53 Rev 4 security controls. The tool will be further enhanced in 2015 to also address the capability to include NIST 800-53 Rev 4 privacy controls in all system security plans, privacy impact assessments, and security controls assessments.

VA is developing a transition plan to move all VA systems currently maintained in the GRC instance at the AITC to the headquarters instance of the GRC. This will enable the VA to have a single GRC system for all VA systems. The effort to have the headquarters instance of the GRC tool updated with capabilities to fully address NIST 800-53 Rev 4 security and privacy controls for all system security and privacy documentation will be completed in the summer of 2015.

Target Completion Date: September 30, 2015

Recommendation 7: We recommend the Executive in Charge 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 last year.)

OIT Response: Concur. The VA Identity, Credential, and Access management (ICAM) PMO is working on establishing a centralized solution utilizing the ICAM AcS system, which will provide for the implementation of mechanisms for enforcing centralized password management policies and standards. The solution will provision user accounts, and provide approval work-flows, self-service functions, and establish Role Based Access Control (RBAC) / Attribute Based Access Control (ABAC) mechanisms for VA users. This will ensure that a standardized password policy is established and implemented for the VA applications, and will provide users self-service capabilities to reset passwords per VA policy. Project implementation of this system is planned for 2016.

The ICAM solution will also provide centralized access management processes to grant authorized users the right to use an application, while preventing access to non-authorized users. For granting access, automatic workflows will be built for approvals by VA supervisors, VA ISOs, and other approval authorities. They will be notified to approve user access requests for integrated systems as well as de-activation of user accounts. The solution will have notifications, delegations, and escalations built in for approving authorities. This will eliminate issues with

unnecessary system privileges, excessive/unauthorized user accounts, accounts without formal access authorizations, and active accounts for terminated personnel.

In the interim while the ICAM solution is implemented, VA has also implemented a process in 2014 for monitoring password policies via predictive scans and remediation processes on OIT systems. Routine system scans are completed by the Network Security and Operations Center (NSOC). An SOP is in place to ensure a structured, repeatable process. Results of the scans are provided to each region for follow-up and remediation of any password weaknesses or deviations from password policies and standards. In 2014, OI&T also updated information system user and system account management policy guidance and processes that emphasized requirements for system owners, systems administrators, and security staff to regularly review the account privileges and access levels for all system users and service accounts. An audit process is in place to conduct quarterly reviews for all system service accounts. Staff members continue to review and adopt servers to allow enforcement of extended password length. The Electronic Computer Access Management (ECAR) system is also being implemented throughout Field Operations. This system is deployed at numerous sites and it minimizes the dependencies on human intervention to process and track access control requirements. Automated functions of ECAR includes: timely termination of accounts, computer access clearance for remote employees, least privilege access account management, validation of background investigation, semi-annual account reviews, elevated privileges review, validation of privacy and information security awareness training, sanitization of accounts for employee transfers, and management of inactive accounts.

Target Completion Date: September 30, 2015

Recommendation 8: We recommend the Executive in Charge 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 last year.)

OIT Response: Concur. As part of the OI&T Security Calendar process used to track and manage recurring security status updates, the Department has implemented reviews of elevated privileges every 90 days and application level access twice a year to ensure the users have minimum system access necessary based on their role. The OI&T Security Calendar is used to track and manage recurring security events and reviews. VA completes a comprehensive review of elevated system privileges, separated users, Common Security Service (CSS) accounts and Consolidated Patient Accounting Center (CPAC) accounts every 90 days. VA also reviews more specific application level access twice a year for Veterans Health Information Systems and Technology Architecture (VistA) menu and security keys to ensure the users have minimum system access necessary based on their role. At each facility, the local ISO and the Chief Information Officer (CIO) work together to identify issues and concerns with staff elevated privileges and, when necessary, engage the 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.

Additionally, a comprehensive review of remote access is done annually and separation of users from VA occur every 90 days. This review, which is also part of the OI&T Security Calendar process, ensures remote access is still authorized and that staff, contractors and volunteers no longer with VA have access privileges removed from e-mail, administrator rights and other VA systems. VistA accounts are automatically disabled for inactivity every 30 days. Active directory accounts automatically disable every 90 days for inactivity. The Department is currently generating the VistA production logs for individuals with elevated system privileges and currently developing a SOP to review the logs, as well as a field implementation plan. The expected completion date is September 2015.

Target Completion Date: September 30, 2015

Recommendation 9: We recommend the Executive in Charge 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 last year.)

OIT Response: Concur. OI&T is developing and has begun partial implementation of a comprehensive risk-based enterprise-wide strategy for audit log collection and review. The strategy will ensure priority resources are reviewing the audit logs for the network infrastructure systems and high risk and moderate risk applications that are most critical to the VA mission. The strategy will also specify more details and refinements to the requirements, policies, and processes that need to be put in place to ensure that VA can effectively analyze and take action on the information and alerts retrieved from the network system and application audit logs. VA has also initiated a multi-phase project that will expand the use of security information and event management (SIEM) solutions and other automated tools to help with the currently manually intensive efforts required to review system and application audit logs.

Enterprise Operations (EO) already has a SIEM solution in place at a number of major VA data centers. The VA NSOC already has a robust audit logging solution. In 2014, Service Delivery and Engineering (SDE) has begun implementing a regional audit logging solution from the VA NSOCs toolset to assist in the collection of logs. The SDE solution is an expansion of the log aggregation and analysis system deployed at the Trusted Internet Connection (TIC) Gateways. Their deployment began in Region 1 in February 2015 and is in production (pilot) at present. Although it is a small scale deployment in that minimal events are being collected, it is allowing VA to assess the feasibility of an enterprise-wide solution. NSOC recently allotted additional licensing to allow SDE to expand this pilot to all regions with an expected completion of summer 2015.

The NSOC is in the process of procuring a SIEM solution to identify and respond to cyber security events in near real-time, for the network devices and security systems that are monitored by the Network Security Operations Center (NSOC), to include VA's Trusted Internet Connection (TIC) gateways, with the award expected in the last quarter of FY 2015. A contract had been awarded for this NSOC requirement in late 2014, but was subsequently cancelled by VA when it was determined that the vendor's solution would not meet the NSOC's requirements. The next phases of the SIEM project in FY 2016 will focus on fielding more robust SIEM solutions and automated tools to collect and analyze audit logs for the regions. The

new target date to complete an enterprise-wide roll-out of SIEM solutions to enable the collection of system audit logs and to conduct centralized reviews of security violations on mission-critical systems is projected for the end of FY 2016, (September 2016).

Target Completion Date: September 2016

Recommendation 10: We recommended the Executive in Charge for Information and Technology implement two-factor authentication for remote access throughout the agency. (This is a repeat recommendation from prior years.)

OIT Response: Concur. Due to the possibility of patient safety issues associated with implementation of the PIV card, implementation for this recommendation within VHA is on hold until care delivery work processes have been developed that accommodate the use of PIV cards by VHA. Implementation of the PIV card for remote access requirements continues throughout the rest of the Department.

In October of 2014, VA coordinated an action plan that discussed a series of options to satisfy the two-factor authentication (2FA) requirement for remote access. In January 2015, VA implemented the selected option based on a phased implementation plan requiring full compliance by all VA personnel by 20 May 2015. At present, 2FA for remote access is 92% complete for Remote Enterprise Security Compliant Update Environment (RESCUE) VPN users by requiring the use of a PIV card to authenticate at the gateway. Technical solutions to support the implementation of 2FA for Citrix Access Gateway (CAG) users are under review and a plan is in place to ensure full implementation and enforcement by the end of the 2015 audit season, September 30, 2015).

Target Completion Date: September 30, 2015

Recommendation 11: We recommend the Executive in Charge 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 last year.)

OIT Response: Concur. VA is able to perform checks and remediation on 100% of RESCUE Government Furnished Equipment (GFE) systems whereas previously no remediation was being performed. This was proven during the FY 2015 efforts to implement Microsoft's MS 15-011 security patch, where VA remediated all systems that had not been patched via IBM Endpoint Manager (IEM) prior to allowing them to connect to VA.

On February 4, 2014, the Deputy Assistant Secretary for Information Security signed a memorandum stating that Personally Owned Equipment (POE) is only allowed to connect through the Citrix Access Gateway (CAG) which provides the necessary protections for the VA network. The CAG provides a Secure Socket Layer (SSL) tunnel between client and Access Gateway located in one of four Trusted Internet Connection (TIC) Gateways. The Access Gateway works like a proxy - all requests by the client are proxied through the Access Gateway

and sent to the respective backend server; therefore, the POE client is never connected to the VA network. Features such as copy/paste are disabled and allowed only by exception.

The original One-VA VPN client was a vulnerable remote access solution. It established an encrypted tunnel but it did not provide any Network Access Controls (NAC) or remediation was not performed prior to connection to VA. This system/service has been decommissioned and no longer poses any risk to the VA network. The decommission of the legacy One-VA VPN took place after a memorandum was issued on July 15, 2014 from the Deputy Assistant Secretary of Information Security.

Target Completion Date: OI&T is recommending that this recommendation be closed - supporting material will be provided under separate cover.

Recommendation 12: We recommend the Executive in Charge for Information and Technology implement more effective automated mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and Web application servers. (This is a modified 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. Plans are in place to continue enhancements the vulnerability management program and processes throughout 2015. The outputs from the scanning tools are broken out and delivered to each data center/region/site. Those sites then annotate those scans with status of the required action, either through remediation, mitigation or issuance of risk based decisions. Priority attention is placed on installing the required patches to remediate the identified deficiencies. Automated monitoring and assessment tools have also been deployed in the VA enterprise to every laptop, desktop, servers and network device.

SDE is collaborating with NSOC to identify databases and prepare for database and web server scanning and remediation. NSOC has developed plans to launch more comprehensive full scale database and web server scans in order to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and Web application servers. In addition to scanning, SDE partners with NSOC to remediate scan findings. Finally, SDE is collaborating with NSOC to utilize Solar Winds/Orion to develop an Internet Protocol registry which will facilitate better device management and ownership/boundary issues. Additional contractor support resources are being applied in 2015 to better enable VA to fully implement the enhanced automated mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and Web application servers

Target Completion Date: December 2015

Recommendation 13: We recommend the Executive in Charge 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 modified repeat recommendation from last year.)

OIT Response: Concur. In February 2013, VA implemented predictive scanning and has continued to build on and improve the patch and vulnerability program to ensure security deficiencies are proactively addressed. VA NSOC added additional personnel to its assessment services team in 2014. These additional personnel have been used to increase the frequency of Open VMS, Database and Enterprise Discovery Scanning. Additionally, VA NSOC has added database scans to the Web Application Security Assessment (WASA) process and worked with SDE to enhance the overall Database scanning processes. VA NSOC has procured additional licensing for Tenable, Appscan and App Detective to support additional scanning requirements. This scanning allows for the identification of vulnerabilities, remediation of those vulnerabilities and compliance monitoring. Monthly predictive scans are tested and remediated, security deficiencies identified and monitored during our assessments of VA's Web applications, database platforms, network infrastructure, and work stations. We receive monthly downloads from our vendors, which are also rigorously tested and monitored to ensure all security deficiencies are identified and remediated. Within Enterprise Operations, a consistent program for identifying and remediating vulnerabilities has been in place for several years.

The predictive scanning process has been augmented with the Nessus Enterprise Web Tool (NEWT) which gathers NSOC monthly and quarterly scans, IEM reports, and System Center Configuration Manager(SCCM); combining them all into one dashboard providing one source of truth of status and reports. In addition, operational NEWT activities have been taking place which include one off scans for IG visits and developing new reporting capabilities, as well as integrating with GRC. In addition, in January 2015, a patch and vulnerability management workgroup convened and created recommendations for streamlining the patch and vulnerability management process. Recommendations were tendered to the executives in charge of Field Operations and OIS and are in the process of being implemented. Additional resources and contractor support are being applied in 2015 that will enable VA to implement a more effective and timely patch and vulnerability management program that will aggressively address security deficiencies identified in VA's Web applications, database platforms, network infrastructure, and work stations.

Target Completion Date: December 2015

Recommendation 14: We recommend the Executive in Charge for Information and Technology implement improved processes for monitoring standard security configuration baselines for all VA operating systems, databases, applications, and network devices. (This is a modified repeat recommendation from last year.)

OIT Response: Concur. Baselines have been created covering the vast majority of systems in the VA Enterprise. Over 95% of the servers in the Department are covered by existing operating system baselines, including all those hosting VA's VistA healthcare application, and virtually 100% of desktops. Existing baselines also cover over 85% of the internetworking devices for VA. Work continues on baselines including defining and establishing database baselines as well as deploying the database baseline establishment. An enterprise triage and coordination of baselines is established and managed by Security Management and Analytics (SMA). SMA coordinates baseline requests including change management, testing, implementation, continuous compliance monitoring and maintaining baseline compliance in conjunction with

OIS. OIS uses IEM tool for security compliance measurement and reporting. Tools are being evaluated for monitoring baseline security compliance of databases, applications, and network devices. Database baselines have been defined, established, and deployed. Work continues for system compliance and remediation, including an in-depth review and documentation of the baseline process, including beneficial enhancements to the process to identify and implement improvements to the way baselines are reviewed and deployed. This will be completed by 9/30/2015.

Target Completion Date: September 30, 2015

Recommendation 15: We recommended the Executive in Charge for Information and Technology implement improved network access controls to ensure medical devices and tenant networks are appropriately segregated from general networks and mission-critical systems. (This is a new recommendation)

OIT Response: Concur. In order to improve medical device isolation, VA is conducting compliance reviews of all Medical Device Isolation Architecture (MDIA) Access Control List (ACL) configurations annually. Additionally, all medical device inventories are certified annually at each VA Medical Center (VAMC). VISN staff is being trained on all of the elements of the medical device security program. Additional controls being implemented include a standardized medical device list based on VA Medical Device Nomenclature Standards, developing an Enterprise Network Connected Medical Device Inventory Database, automating the inventory of devices behind MDIA ACL's every 90 days using the database, and adding medical devices to the existing GSS inventory.

In February 2015, VA issued updated security requirements and guidance for network connected medical devices and systems. This updated guidance was developed through the efforts of the Medical Device Protection Program Leadership Working Group, and served to strengthen the security and network access controls in place to isolate and better protect medical devices attached to VA networks, and to ensure that medical devices are appropriately segregated from general networks and mission-critical systems. Tenant systems and financial systems are currently being evaluated to determine the level of segregation that would be appropriate to ensure that tenant networks are securely segregated from general networks and mission-critical systems. In the short term, VA is adding additional security monitoring of the financial systems via the SIEM system. For the long term, VA will pursue an intelligent NAC solution that will be more effective than traditional firewall segregation. This NAC solution will be able to granularly control both traffic and user access to financial and tenant systems.

Target Completion Date: September 2015 for medical devices, and September 2016 for tenant systems.

Recommendation 16: We recommended the Executive in Charge for Information and Technology consolidate the security responsibilities for tenant networks present under a common control for each site and ensure vulnerabilities are remediated in a timely manner. (This is a new recommendation)

OIT Response: Concur. VA is continuing to improve security by ensuring these tenant systems are identified along with the responsible organizations and are held to the same security standards as other systems. All tenant systems vulnerabilities are being identified in the vulnerability management systems that VA has implemented to assist in remediation efforts. These systems clearly show organizational responsibility for remediation efforts. In addition, the data centers have instituted a tenant hosting program that clearly lays out security responsibilities for customer managed systems and is requiring those customers to sign a Rules of Behavior document acknowledging their responsibilities. All systems at data centers are reviewed at bi-weekly CRISP Integrated Project Team meetings, and systems that are not remediating according to guidance are required to explain any issues directly to executive leadership.

Target Completion Date: OI&T is recommending that this Recommendation be closed - supporting material will be provided under separate cover.

Recommendation 17: We recommend the Executive in Charge 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 modified repeat recommendation from last year.)

OIT Response: Concur. In 2009, OI&T Product Development (PD) and Service Deliver and Engineering (SDE) jointly implemented change and configuration management governance over software and system controls and issued VA policy and procedures. PD implemented Change and Configuration Management Plans (ChM/CfM) and tools for all software projects to formalize standardized software and artifact change management controls. PD implemented tools to be standardized to manage source code and document change and version control. PD includes configuration managers as necessary project team members when activating new software development projects. PD implemented change control boards at the program level to oversee requirements for change. PD implemented standardized requirements management and software testing tools to enable requirements traceability capabilities and requirement change/design change/test case change traceability is documented. PD is working with OIS to implement security vulnerability testing tools to be used prior to software release to test specifically for security requirements compliance. PD implemented Integrated Project Teams to determine compliance and readiness acceptance with internal customer requirements. PD includes compliance with security and configuration management processes in milestone review criteria.

Through a highly active Integrated Project Team (IPT) of Change Management subject matter experts, OI&T is improving the change control framework including the integration of information security. This team has ensured the existence of an Enterprise Change Management SOP that incorporates security impact analysis. With the Enterprise Change Management SOP in place, the team is remediating organizational level Change Management SOPs including those of PD, Field Operations (FO), Enterprise Systems Engineering (ESE), EO, and NSOC to ensure that they meet the guidelines of the Enterprise Change Management SOP. The team has also implemented Change Management training which includes 3 courses that will be mapped in the Change Management Competency Model. This team will complete the Change Management

improvements by early summer of 2015. In FY15 PD has confirmed procedures for Test Plans, Configuration Management, and Release Management are in place. PD has committed to increasing the training and awareness of Configuration Management (Test, Change, and Release).

Target Completion Date: June 30, 2015

Recommendation 18: We recommend the Executive in Charge for Information and Technology implement processes to ensure information system contingency plans are updated with the required information. (This is a modified repeat recommendation from last year.)

OIT Response: Concur. The OIG noted the progress that VA has made with contingency plans and the testing of contingency plans. VA has continued to make improvements in this area in 2014 and early 2015, as processes were re-validated and updated to ensure information system contingency plans are updated with the required information. OIT has published VA handbook 6500 and VA Handbook 6500.8 which provides the guidance for contingency plans specified by the National Institute of Standards and Technology (NIST). The guidance includes the standardized processes and templates for contingency plans. The Office of Business Continuity within OIS monitors and provides daily and monthly progress reports on the compliance status of contingency plans and disaster recovery plans for VA systems with the guidance. Information system contingency plans and other related plans were specifically reviewed for accuracy in 2014, and updates were made to include all required information.

VA also made use of the Annual Security Calendar in 2014 and 2015 to develop action items requiring that all Information System Contingency Plans and Disaster Recovery Plans be reviewed and updated on an annual basis to more accurately reflect system accreditation boundaries, and roles and responsibilities. Organizational re-alignments such as the FY 2015 MyVA Regional re-alignment may result in a number of additional changes to system accreditation boundaries, which may also impact the content of the contingency plans. The OIS Office of Business Continuity is obtaining additional contractor support in the third quarter of FY 2015, to conduct an independent review and re-validation of all Information System Contingency Plans to further ensure that all VA Information System Contingency Plans are updated with the required information. The effort is viewed as an ongoing requirement for VA, as we will continue updating any plans that need to be updated for accuracy due to boundary changes and possible organizational re-alignments.

Target Completion Date: September 30, 2015

Recommendation 19: We recommend the Executive in Charge for Information and Technology develop and implement a process for ensuring the encryption of backup data prior to transferring the data offsite. (This is a repeat recommendation from prior years)

OIT Response: Concur. In response to this need, VA has identified high level requirements for an Enterprise level Tape Backup Encryption solution, and programmed funding. We have assigned a program team lead, and have begun the discovery process for requirements of an enterprise wide solution to address this issue.

To address the defect and mitigate risk in the near term, a full review was conducted on the risk and a Risk Based Decision (RBD) was implemented. This national RBD identifies mitigating controls to compensate the lack of backup tape encryption and is further documented in local security documentation for systems that do not support backup tape encryption, at present. VA believes that the mitigating controls and processes are adequately addressing the risks at sites that do not support backup tape encryption.

Early last year (2014) we convened an Enterprise VistA Backup Encryption Work Group to conduct an in depth review of this issue and recommend a solution. We determined that not all VistA systems outside of the DISA datacenters were encrypted. A contract for encryption hardware and software was awarded, equipment and software purchased, and installed and operational by end of December, 2014, encrypting all VistA system Backups. VA is continuing efforts to assess its current processes for ensuring that proper security mechanisms and controls are in place to protect backup data prior to transferring the data offsite for storage.

Due to the high costs associated with encrypting all back-up media throughout all VA locations, VA has pursued a risk-based approach that enables the Department to continue the use of enhanced physical security mechanisms and maintain positive control of back-up tapes and other back-up storage media. A comprehensive review to ensure proper security controls are in place to protect back-up tapes and other back-up storage media will be conducted in the third and fourth quarters of FY 2015. VA will identify the specific locations where it can cost-effectively implement the encryption of backup data prior to transferring the data offsite for storage, while also continuing to ensure adequate and cost-effective security controls and processes are in place at all other VA locations to secure backup storage media that is transferred offsite for storage.

Target Completion Date: December 30, 2015

Recommendation 20: We recommend the Executive in Charge 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 last year.)

OIT Response: Concur. In March 2014, the NSOC initiated an Incident Response (IR) Working Group to review current cyber security incident response policies, procedures and performance measures. The working group provided recommendations on improvements to our cyber security IR capability. One product from this group was an Executive Decision Memo (dated 26 March 2014) mandating field personnel to adhere to the NSOC timelines (e.g. immediately for confirmed compromised hosts, within 48 hours for host scan requests, and within 72 hours for reimaging of hosts) upon direction from the VA-NSOC. The NSOC has updated the NSOC Incident Response Plan (March 6, 2015).

The NSOC and Field Security Services (FSS) have implemented new Daily Open Ticket Reports (DOTR) along with a recurring daily meeting to discuss and update every ticket. This has resulted in the time from ticket creation to remediation from an average of 17 days to 2 days.

OIS has also worked with SDE on better communications and resolution of cyber security incidents. OIS is also set to award a contract for a new ticketing system which will integrate with the VA's National Ticketing System within FY15. This new system will allow for VA NSOC, ISOs, and IT support staff to all see the same cyber security incident information and remediate the tickets which cannot be done at this time due to disparate ticketing systems. This will also provide a more efficient incident response process reducing time to remediation.

The NSOC successfully completed a United States Computer Emergency Response Team (USCERT) Incident Response Exercise on November 18, 2014 and will continue to leverage USCERT assessments to increase efficiencies. The Department of Homeland Security will also be conducting an assessment of the NSOC Incident Response during the week of April 20, 2015. The NSOC worked with the IT Workforce Development office to develop the NSOC Cyber Security Competency Model in the VA Talent Management System (TMS). The competency model is currently used by all NSOC personnel. OI&T will ensure that role based security incident response training is included in Individual Development Plans, and completed by the appropriate incident response personnel. 100% of NSOC government staff with incident response responsibilities completed the USCERT Incident Handling Class during January of 2015.

Target Completion Date – September 30, 2015

Recommendation 21: We recommend the Executive in Charge for Information and Technology identify all external network interconnections and implement improved processes for monitoring VA networks, systems, and exchanges for unauthorized activity. (This is a modified repeat recommendation from last year.)

OIT Response: Concur. VA has made good progress in addressing this recommendation throughout 2014 and recommends closure of this recommendation. All external network interconnections are monitored for unauthorized activities. All external network connections fall into one of four categories: Site to Site VPN connections (S2S), LAN Extensions (LANEX), Business Partners Extranets (BPE), and Business Partner Gateways (BPG). All four varieties are monitored and logs are collected and fed into the "Splunk" system for analysis and review.

A S2S VPN enables a VA Business Partner to securely access specific resources on the VA WAN. It does this by establishing a VPN connection between the Business Partner network and one of the TIC Gateways. Traffic that may pass over this connection is limited, so only specific VA and Business Partner systems may communicate with each other. S2S VPNs are afforded the protections, monitoring, and logging provided by the TIC architecture. A LAN Extension enables a secure VA facility to communicate with the VA Wide Area Network by way of an internet connection. It does this by establishing a VPN connection between the facility and one of the TIC Gateways. LANEXs are similar to the S2S's in that they are afforded the protections, monitoring, and logging provided by the TIC architecture.

A BPE is an encrypted connection between a remote party (Business Partner, Vendors, affiliate university, etc.) and VA through one of the VA TIC Gateways. BPE uses a leased circuit that directly connects the two partners and is therefore capable of supporting higher bandwidth

requirements. There is a firewall and IPS inline between the partner facility and the VA WAN that is monitored and logging is sent to "Splunk" for review and analysis as well as all internet traffic traverses the TIC and leverages the technologies within the TIC stack.

A BPG is a direct connection between a non-VA facility and the internal VA network. It is used to carry high volume and/or time sensitive data that exceeds the practical capacity of the VA WAN. A BPG provides access only to the VA facility where the BPG is connected. The Business Partner Gateways do not traverse the TIC but do have a VA Firewall and VA IBM ISS Intrusion Prevention System with all logs being aggregated at the SiteProtector Central Repository and the NSOC's "Splunk" implementation. These connections are monitored and logs are analyzed and reviewed. All Memoranda of Understanding (MOU) and Interconnection Security Agreements (ISA) for known external network connections have been reviewed (as part of OI&T's annual review) and updated to reflect operational environments. This review process is now part of an annual cycle. OI&T has documented these known connections and has also published guidance on this subject.

Target Completion Date: OI&T is recommending that this Recommendation be closed - supporting material will be provided under separate cover.

Recommendation 22: We recommended the Executive in Charge for Information and Technology implement and monitor incident response metrics to assist in tracking and remediating all cybersecurity events. (This is a new recommendation)

OIT Response: Concur. In March 2014, the NSOC initiated an IR Working Group to review current cyber security incident response policies, procedures and performance measures. The working group provided recommendations on improvements to our cyber security IR capability. One product from this group was an Executive Decision Memo (dated 26 March 2014) mandating field personnel to adhere to the NSOC timelines (e.g. immediately for confirmed compromised hosts, within 48 hours for host scan requests, and within 72 hours for reimaging of hosts) upon direction from the NSOC. The NSOC has updated the NSOC Incident Response Plan (March 6, 2015). The VA Handbook 6500 was also updated and signed (March 10, 2015).

The working group also established performance metrics to measure the effectiveness of the incident response activities, and has already worked to incorporate new metrics into the May 2014 OI&T Performance Review (OPR). The NSOC has worked diligently in getting new performance metrics implemented into the current ticketing system. These metrics and reports are to be completed by 30 June 2015. New metrics that are being developed and implemented are: All CAT 1 reported to USCERT within 1 Hour, Master Ticket Creation and Remediation/Closure, CAT3 Ticket Creation and Remediation, VA NSOC Triage Metrics. The NSOC has also started tracking the time from ticket creation to ticket closure.

The NSOC is also diligently working on implementing the new USCERT classifications and reporting requirements into the existing ticketing system. These new classifications are required to go into effect September 30, 2015. OIS is also set to award a contract for a new ticketing system which will integrate with the VA's National Ticketing System in FY15. This new system will allow for the NSOC, ISOs, and IT support staff to all see and remediate the tickets

without utilization of disparate systems. The new reporting metrics will also be implemented for better tracking of all cyber security incidents from identification through remediation.

Target Completion Date – September 30, 2015

Recommendation 23: We recommend the Executive in Charge for Information and Technology develop a listing of approved software and implement continuous monitoring processes to identify and prevent the use of unauthorized application software, hardware and system configurations on its networks. (This is a modified repeat recommendation from last year.)

OIT Response: Concur. OI&T has established a cross functional group that has developed a SOP for the removal of unauthorized software across the enterprise. The SOP has been put into pilot production as of March 2015. To establish a baseline of software assets and versions currently deployed, the Unauthorized Software working group has acquired a software asset normalization tool. This tool will import the discovery scans from IEM and SCCM and normalize the data to assist the removal process. Those items identified and required to support VA's mission will be submitted to the Technical Reference Model (TRM) for adjudication. The TRM has been designated the authoritative source for software and hardware assets. The TRM will continue to evolve as the discovery scan data is analyzed and submitted for decision. Currently, the IEM tool has identified approximately 59,000 software titles across the enterprise requiring evaluation, prioritization, and business justification. Implementation for continuous monitoring to prevent use of unauthorized is still underway.

The workgroup has established a VA-wide communications plan to educate VA end users on the importance of not installing unauthorized software on the VA network. The initial communications was published in 13 communications channels across VA covering all administrations. To assist in the prevention of installing unauthorized software, the DAS for Information Security and the Deputy Chief Information Officer for SDE jointly signed an Elevated Privileges Guidance Memorandum providing the process for requesting elevated privileges based on the type of access needed to perform your position requirements. A comprehensive review and reporting of Elevated Privileges is ongoing.

VA deployed the Software Use Analysis to provide the foundation for holistic software asset management by discovering all licensed and unlicensed software with in-depth granularity across all devices via the IEM tool across all Windows devices. It serves as a key element of VA's continuous monitoring program as IEM is used to identify unauthorized application software, hardware, and system configurations on VA networks. A plan has been developed that includes development and implementation of processes and solutions to prevent the use of unauthorized software, and to remove unauthorized software on VA networks. Additional contractor resources are planned for 2015, to assist VA in resolving this IG Recommendation.

Target Completion Date: December 30, 2015

Recommendation 24: We recommend the Executive in Charge 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 last year.)

OIT Response: Concur. During FY14, VA developed and deployed the VA Systems Inventory (VASI) to establish the authoritative source of VA systems. VASI provides a comprehensive repository of basic information about VA systems (both major and minor applications as defined by FISMA) and represents the relationships between systems and other key VA data stores. VASI and the data necessary to fully describe systems will continue to mature during FY15 and beyond, but the inventory has been broadly accepted and is integrated into existing governance processes to ensure information is kept current and accurate.

VASI and the data necessary to fully describe systems will continue to mature during FY15 and beyond, but the inventory has been broadly accepted and is integrated into existing governance processes to ensure information is kept current and accurate. As the information in VASI continues to evolve, VA's ability to accurately understand the relationships between systems, infrastructure, data, programs, business process, strategic goals and other areas will be enhanced resulting in improved enterprise level decision making. The office of Architecture, Strategy and Design, Enterprise Architecture has drafted a policy establishing VASI as the "System of Record" for VA Systems and defines the objectives, principles, roles and responsibilities for the utilization, management and sustainment of the VASI. The draft policy is being finalized and will be submitted to VAIQ for formal concurrence. The VASI is accessible to VA users at: http://vaww.ea.oit.va.gov/va-systems-inventory/

Target Completion Date: June 30, 2015

Recommendation 25: We recommend the Executive in Charge 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 modified repeat recommendation from last year.)

OIT Response: Concur. VA 6500.6 provides guidance regarding oversight of contractor managed systems. Consistent with this policy, VA requires managed service providers to comply with these standards, inclusive of supporting on-site Security Controls Assessments (SCAs) and allowing routine compliance monitoring by the NSOC. To address this concern, the Technical Acquisition Center (TAC) incorporated language into Performance Work Statements that requires the contractor to preserve such data, records, logs and other evidence which are reasonably necessary to conduct a thorough investigation of any computer security incident. The contractor is also required to fully cooperate with all audits, inspections, investigations, or other reviews conducted by or on behalf of the Contracting Officer or the agency's Office of Inspector General. The contractor must provide full and free access of the following to the Contracting Officer, designated representative of the Contracting Officer, and representatives of the agency's Office of Inspector General: the Contractor's (and Subcontractors') facilities, installations, operations documentation, databases, and personnel used for contract hosting services.

In December of 2014, the Senior Acquisition Executive issued guidance to all VA offices to review all existing contracts that provided contractor hosted environments for VA systems to ensure all of those contracts included all requirements for FISMA compliance. This review was completed at the end of 2014 and VA's annual security controls assessment processes include reviews of contractor hosted environments to ensure that the contractor's security controls adequately protect VA sensitive systems and data. A longer term solution specific to contractor-managed cloud-based systems is the development of "Cloud Computing" related clauses, to be required to go through formal rulemaking. The proposed "Cloud Computing" clause and optional clause paragraphs impose substantial new burdens on contractors and the public, as well as including substantial record-keeping requirements on contractors and strict notification requirements to the government (such as reporting security incidents). OI&T will work with the Office of Acquisition, Logistics and Construction to develop a long-term clause solution. VA is also developing a Cloud Strategy which will also address requirements for procedures for overseeing contractor-managed cloud-based systems and ensuring information security controls in the cloud adequately protect VA sensitive systems and data.

Target Completion Date: December 2015

Recommendation 26: We recommend the Executive in Charge for Information and Technology implement mechanisms for updating the Federal Information Security Management 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 is continuing to improve efforts towards improving the accuracy of its FISMA inventory of systems. VA is reviewing any gaps in 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. The system inventory, maintained by GRC, is reviewed continuously by the Risk Vision Working Group and by OIS management. Completed annual reviews are moving to a monthly validation of systems in the inventory to ensure they are assigned to the proper accreditation boundary. VA is also developing updated guidance related to security requirements for the accounting for 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.

Target Completion Date: September 30, 2015

Recommendation 27: We recommend the Executive in Charge for Information and Technology implement mechanisms to ensure all users with VA network access participate in and complete required VA-sponsored security awareness training. (This is a repeat recommendation from last year.)

OIT Response: Concur. VA recommends closure of this finding as we have fully implemented the necessary mechanism to ensure all users with network access take and complete Security & Privacy Awareness Training and sign National Rules of Behavior on an annual basis. For FY

2014 and through the first 5 months of FY 2015, VA is averaging over 98% compliance for this requirement to include, employees, contractors, residents, trainees, and eligible volunteers against a target of 96%. Out of a user population of over 500,000 people, the less than 2% not current in their training has no statistical significance or materiality. This percentage results primarily from the continuous turn-over in TMS and PAID creating a lag time in on-boarding and off-boarding users. A 100% compliance rate is never achievable and is an unrealistic and impossible standard. The extremely small number of users found in non-compliance are outliers and not indicative of a systemic problem as indicated by this finding.

VA has fully implemented an automated process to track this training, and since March of 2013, VA no longer uses or relies on any manual processes to track the fulfillment of this training requirement. Starting in March of 2012, VA, at the direction of the then Deputy Secretary, mandated that only TMS serve as the repository for training certification. VA also mandated that by March of 2013 all users migrate to TMS on the anniversary of their training requirement. TMS employs an automated notification system to users and their supervisor or COR. These changes are codified in VA Directive 0004 – April 2012, which states that the directive strengthens VA's ability to more accurately track training and reduce the risk of non-compliance with FISMA and its requirement for security awareness training for Department personnel, including contractors and other users of VA information systems. This directive also supports CRISP by establishing the VA TMS as the official system for completing, recording and reporting VA mandatory annual FISMA compliance training.

Directive 0004 also states that the directive "consolidates all VA learning management activities into the official TMS for all audiences (VA employees, without compensation employees (WOC), contractors, volunteers and Veteran Service Organization (VSO) representatives, residents, and trainees)." VA continues to improve its on-boarding and off-boarding processes which will result in an even higher compliance percentage greater than the 98% it currently has. The small numbers of users who may be in non-compliance is not indicative of VA's success in ensuring one of the highest compliance rates in the federal government. If, after ample notification (and in compliance with the master agreement VA has with employee unions), a user still fails to take all required training, the local CIO will disable the user's account until compliance is obtained. There is a policy in place, the process is automated, and no manual tracking of compliance is sanctioned or tolerated in the unlikely event it is still used anywhere in the VA system.

Target Completion Date: OI&T is recommending that this recommendation be closed - supporting material will be provided under separate cover.

Recommendation FY 2013-27: We recommended the Executive in Charge for Information and Technology develop guidance and procedures to integrate information security costs into the capital planning process while ensuring traceability of Plans of Action and Milestones remediation costs to appropriate capital planning budget documents.

OIT Response: Concur. To ensure that VA adequately plans and funds security remediation efforts identified during the Authorization & Accreditation (A&A) process, OI&T has developed the SOPs requiring the formal inclusion of all POA&Ms generated by the GRC tool in OI&T's

Planning, Programming, Budgeting, and Execution (PPBE) process. The PPBE process provides traceability from projects, up through programs and into investments (the latter captured as Exhibit 300s and colloquially referred to as the Capital Planning and Investment Control [CPIC] process). A separate policy directive instructing POA&M developers how to enter their material into the PPBE process for programmatic and funding consideration has also been developed. Both processes when executed together provide funding traceability from POA&M through PPBE and into CPIC (Exhibit 300s) capital planning and budget documents. These updated procedures have been completed and are being distributed by May 2015.

Target Completion Date: May 2015

Recommendation FY 2010-21: We recommended the Assistant Secretary for Information and Technology develop mechanisms to ensure risk assessments accurately reflect the current control environment, compensating controls, and the characteristics of the relevant VA facilities.

OIT Response: Concur. OI&T recently signed and distributed a new version of VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3. VA Information Security Program," which is based on NIST Special Publication 800-53 Revision 4. This revised handbook brings the Department's security policy into full compliance with Federal requirements for an agency-wide risk management framework and governance structure. Governance is provided in the "Roles and Responsibilities" section of this handbook. OI&T has also implemented the GRC tool as a major element of implementing an agency-wide risk management governance structure. The GRC tool is VA's robust repository capable of tracking the real-time security posture of the VA's IT systems and provides the mechanism to identify, monitor, and manage risks across the enterprise.

The tool is used in concert with existing IT monitoring and tracking tools, such as IEM, Solar Winds, and NESSUS, to extract, in real-time, up to 54 NIST controls, while capturing the remaining controls via automated workflows. The Risk Vision GRC tool automatically ties risk assessments to POA&Ms and system security plans, resulting in a more comprehensive understanding of VA's security posture, far exceeding any past capabilities. The workflow process of entering information into the GRC tool ensures that only the most current risk information is retained. This is also true of the System Security Plan and FIPS assessments. The CIO has greater visibility/oversight with the Risk Vision database for ATO decisions. OI&T maintains a mature ERM organization that proactively manages risks that are applicable to the OIT enterprise. Within ERM, the RAM office has an IT Security and Compliance Risk Division that is focused on the assessment and mitigation of information security risks that meet the organization's definition of enterprise-level risk. OIS also has a Risk Management office that addresses information security risks that do not rise to the level of OIT enterprise risks.

Target Completion Date: OI&T is recommending that this recommendation be closed - supporting material will be provided under separate cover.

Recommendation 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.

OIT Response: Concur. VA, like other Federal agencies, is mandated to use the Office of Personnel Management's Position Designation System and Automated Tool (PDT) to review position descriptions and statements of work. Once the designation has been made, the requisite background investigation is conducted. In efforts to help promote the update of 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, the updated version of VA Directive 0710 requires the use of the PDT. To provide updated guidance, PSS revised the VA 0710 Handbook, which is in draft and will be available for staffing by the end of April 2015.

VA also requires each Servicing Human Resources Office to review and certify position descriptions every two years. Part of this review, besides validating series and grade, is to revalidate the position designation. Again, this revalidation is done utilizing PDT. The onboarding solution, utilizing the IAM AcS system, will facilitate automated processes to track "Rules of Behavior" and annual privacy trainings for VA users. The solution will be integrated with TMS to track training requirements and compliance. In a case where a user record is not compliant with the VA policy of taking the proper trainings, the user account will be de-activated until proper actions are taken. IOC for this system is November 2016.

Target Completion Date: November 2016

Recommendation 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.

OIT Response: Concur. VA has developed an onboarding solution, utilizing the ICAM AcS system, which will establish appropriate business rules based on the position description and the sensitivity to conduct investigations and re-investigations. For example, when a new employee joins VA with a high risk designation, the solution will receive the appropriate user attributes from HR-Smart to create an account within the onboarding solution. The onboarding solution will then use the high risk applicability attribute to determine if a background investigation is required. In this case, the user has a high risk position sensitivity requiring a Background Investigation (BI). These investigation data attributes will be sent to PSSS to trigger the correct investigations with OPM. The IOC for this system is November 2016.

At the 4.5 year mark, a system generated message will be sent to the PSSS application to initiate the re-investigation process. This will minimize the number of individuals with outdated investigations. The PSSS V 1.0 configuration is due for release on or about June 1, 2015. PSS continues to collaborate with facility Servicing Human Resources Office to review their

employee background investigation data. This review will include comparing the position designation with the background investigation. If the investigation is not at the required level, a new investigation is initiated. This review will also produce the reinvestigation results. Since the audit is reviewing the data of the previous investigation, investigations that are out of scope for their periodic reinvestigation are identified and action is taken to rectify the deficiency.

As a process improvement, an automated tool was developed and implemented in March 2015 that will enable more frequent recurring audits. At the present time, OPM does not require reinvestigations for those employees at the Moderate Risk positions. OPM is delaying the implementation of the reinvestigation requirement until the new 5 CFR 1400 is signed and approved.

Target Completion Date: November 2016

Recommendation 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.

OIT Response: Concur. VA developed Directive 6512, Secure Wireless Technology and Wireless Security, to supplement VA Handbook 6500. The Directive provides guidelines for protecting VA wireless networks from signal interception, enhancing network security, and segmenting VA's wireless network from the wired network. VA has replaced 88% of the legacy wireless networks with more robust and secure wireless networks, defining strict configuration guidelines and implementation plans. VA will be at 99% by October 31, 2015 for the remainder of the current installations. VA established the National Wireless Infrastructure Team to ensure all authorized VA wireless access points use a standard wireless network configuration. Rogue Access Point detection technology is part of the rollout and VA is working to design a comprehensive approach to identifying and shutting off threatening Access Points.

VA established a contract to conduct wireless scanning of a percentage of VA sites annually. These scans are comprehensive in nature and designed to scan for open, rogue, or unsecured AP's within the facility; look for other electronic devices and verify and document if these devices cause Radio Frequency Interference (RFI) on the WLAN; and capture data information such as source and destination MAC address, features enabled on the client, features enabled on the access point, supported transmit speeds, current transmit channel, encryption status, SSID, beacon interval, and all pertinent data. Further, the effort will be designed to reduce threats and mitigate vulnerabilities associated with the scanned VA facility's wireless networks. All sites within VA will ultimately be assessed as part of this effort.

Target Completion Date: October 2015

Recommendation 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.

OIT Response: Concur. In September 2014, VA completed the deployment for GETVPN encryption of sensitive data transmitted over Multi-Protocol Label Switching (MPLS) circuits in response to VA OIG and FISMA recommendations and VA CIO direction. Once that work was completed, VA leadership continued the internal encryption build out with GETVPN implementation on localized Point-to-Point circuits such Single and Multi-links and Metro-e links. The effort to encrypt the balance of VA circuits led to the creation of the GETVPN Acquisition Installation and Activations project on 10/28/2014. Currently the GETVPN project is in Planning Phase of Project Management Accountability System (PMAS). It is projected that VA's efforts to resolve clear text protocol vulnerabilities will not complete until December 2015.

Target Completion Date: December 2015

Appendix E Office of Inspector General 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

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.