VA Office of Inspector General

OFFICE OF AUDITS & EVALUATIONS

# Department of Veterans Affairs

*Federal Information Security Management Act Audit for Fiscal Year 2013*

**May 29, 2014**
**13-01391-72**

# ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| CRISP | Continuous Readiness in Information Security Program |
| DHS | Department of Homeland Security |
| FISMA | Federal Information Security Management Act |
| FY | Fiscal Year |
| 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 | Veterans Affairs |

# Department of Veterans Affairs

# Memorandum

Date: May 15, 2014

From: Assistant Inspector General for Audits and Evaluations (52)

Subj: VA's Federal Information Security Management Act Audit for Fiscal Year 2013

To: Executive in Charge for Information and Technology (005)

1. Enclosed is the final audit report, *Federal Information Security Management Act Audit for Fiscal Year 2013*. 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) 2013 audit of VA's consolidated financial statements.
- 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 2013.

5. This report provides 35 recommendations for improving VA's information security program; 30 recommendations are included in the report body and

5 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 information about security policies and procedures was not finalized or information security control deficiencies were repeated during the FY 2013 FISMA audit. CliftonLarsonAllen LLP examined whether VA's corrective actions successfully addressed the outstanding recommendations.

6. The effect of these open recommendations needs to be considered in the FY 2014 assessment of VA's security posture. We remain concerned that continuing delays in implementing effective corrective actions to address these open recommendations can potentially contribute to reporting an IT material weakness from this year's audit of VA's Consolidated Financial Statements.

7. Our independent auditors will follow up on the outstanding recommendations and evaluate the adequacy of corrective actions during the FY 2014 FISMA audit.

LINDA A. HALLIDAY

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

April 18, 2014

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, 2013 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 2013 through November 2013. 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.

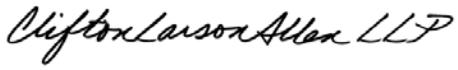
We performed limited reviews of the findings, conclusions, and opinions expressed in this report that were related to the financial statement audit performed by CliftonLarsonAllen LLP. The financial statement audit results have been combined with the FISMA performance audit findings. We do not provide 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 2013. 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: VA's Federal Information Security Management Act Audit for Fiscal Year 2013

## 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 FY 2013 audit determined the extent to which 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, FISMA audits continued to identify significant deficiencies related to access controls, configuration management controls, continuous monitoring controls, and service continuity practices designed to protect mission-critical systems.

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

Further, VA has not remediated approximately 6,000 outstanding system security risks in its corresponding Plans of Action and Milestones to improve its overall information security posture. As a result of the FY 2013 consolidated financial statement audit, CliftonLarsonAllen LLP concluded 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 generally agreed with our findings and recommendations. We will monitor implementation of the corrective action plans.

LINDA A. HALLIDAY
Assistant Inspector General
for Audits and Evaluations

# TABLE OF CONTENTS

# 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) 2013 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 79 major applications and general support systems at 24 VA facilities. As noted in last year's FISMA report, 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. Security Capital Planning
9. Contractor Systems Oversight
10. Security Awareness Training

This report provides 35 total recommendations, including three new recommendations, for improving VA's information security program. Thirty recommendations are included in the report body and five 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 2012 FISMA report provided 32 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, FISMA audits continue 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-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* issued in November 2013, provides guidance for Federal agencies to follow in meeting 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. 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 status. As a result of the CRISP initiative, we noted improvements related to:

- Providing consistent training for both role-based and security awareness
- Testing contingency plans
- Reducing the number of individuals with outdated background investigations
- Improving data center Web application security

- 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

However, these controls require time to mature and show evidence of their effectiveness. Accordingly, we continue to see 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 made progress updating risk management policies and procedures, our FISMA audits identified deficiencies related to VA's risk management strategy, Plans of Action and Milestones (POA&Ms), and system security plans—all are discussed in the following section. Each of these processes is vital 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 communicated to the data centers, regional offices, and medical facilities we visited. Additionally, VA has not ensured that its information security controls are effectively monitored on an ongoing basis to include documenting significant changes to the system, conducting security impact analyses for system changes, and reporting system changes to designated organizational officials. Risk assessments were not properly updated as they included references to inaccurate system environment information. Further, some security self-assessments were not performed annually in accordance with FISMA requirements.

NIST SP 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 recently updated its VA Handbook 6500 to provide guidelines on how to comply with revised risk management requirements. Additionally, VA is implementing a risk governance structure, including a Risk Management Governance Board, to monitor system security risks and implement risk mitigation controls across the enterprise. Until this effort is complete, enterprise-wide risks may not be 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*, 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 6,000 open POA&Ms in FY 2013 compared with 4,000 open corrective actions in FY 2012. POA&Ms identify which actions must be taken to remediate system security risks and improve VA's information security posture.

VA did not include prior year information security POA&Ms within its legacy central reporting database because of a planned transition to a new centralized Governance, Risk, and Compliance monitoring and reporting system. In the interim, the Office of Information Technology established a SharePoint site to track prior year findings and corrective actions. However, VA does not have an accurate representation of total POA&Ms since it has not added any new corrective actions to its central database since March 2012.

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, 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 that still remain as the underlying weaknesses have not been fully remediated.

POA&M deficiencies resulted from a lack of accountability for closing items and a lack of controls to verify supporting documentation had been added to the central database. Furthermore, unclear responsibility for addressing POA&M records at the "local" level continues to adversely affect remediation efforts across the enterprise. By failing to fully remediate significant system security risks in the near term, VA management cannot ensure that information security controls will protect VA systems throughout their life cycles. 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***

Audit teams continue to identify system security plans with inaccurate information regarding operational environments including system interconnections and compensating information security controls. VA Handbook 6500, Appendix D provides guidelines on maintaining and updating system security plans for major applications and general support systems. 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 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 last year.)*

2. We recommended the Executive in Charge for Information and Technology implement mechanisms to ensure sufficient supporting documentation is captured in the central database to justify closure of Plans of Action and Milestones. *(This is a repeat recommendation from last year.)*

3. We recommended the Executive in Charge for Information and Technology define and implement clear roles and responsibilities for developing, maintaining, completing, and reporting Plans of Action and Milestones. *(This is a repeat recommendation from last year.)*

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 last year.)*

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 interconnection and ownership information. *(This is a 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, security impact analyses, and security self-assessments on at least an annual basis and ensure all required information accurately reflects the current environment. *(This is a repeat recommendation from last year.*

## Finding 2 Identity Management and Access Controls

Audit teams identified significant deficiencies in VA's identity management and access controls. VA Handbook 6500, Appendixes D and 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 audit teams continued to identify multiple password management vulnerabilities. For example, the teams found 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 D 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 employees. 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 eliminate instances of unauthorized system access and 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 D 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.

***Remote Access***

VA lacks a consistent process for managing remote access to VA networks. VA does not have policies that provide reasonable assurance of restricting privileged remote access from foreign countries that may pose a significant security risk to VA systems. In addition, multi-factor authentication for remote access has not been fully implemented across the agency. VA Handbook 6500, Appendix D 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, applications, and network devices. *(This is a repeat recommendation from last year.)*

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 excessive or unauthorized accounts. *(This is a modified repeat recommendation from last year.)*

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 last year.)*

10. 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 last year.)*

11. 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 last year.)*

12. We recommended the Executive in Charge for Information and Technology develop and implement policies and procedures for restricting privileged remote access from foreign countries that may pose a significant security risk to VA systems. *(This is a new recommendation.)*

## 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 D provides high-level policy guidelines regarding mandatory configuration settings for information technology hardware, software, and firmware. However, testing 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 "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 audits 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 1, *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 audits 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, Version 2, *Creating a Patch and Vulnerability Management Program*, 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.

***Baseline Security Configurations***

VA is developing 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 on all VA systems. For example, testing at VA facilities revealed varying levels of compliance, ranging from 78 to 98 percent, with United States Government Configuration Baseline standards for end-user systems. Testing also identified numerous network devices not configured to a common security configuration standard, resulting in default network services, excessive permissions, weak administrator passwords, and 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

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

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

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

## Finding 4 System Development/Change Management Controls

VA has not fully implemented procedures to enforce standardized system development and change management controls for mission-critical systems. Our audit teams continued to 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.

Further, numerous test plans, test results, and approvals were either incomplete or missing. 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

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

## Finding 5 Contingency Planning

Overall, we noted an improvement in contingency plan testing since our FY 2012 audit. However, VA contingency plans still were not fully documented and test results were not consistently communicated to senior management. VA Handbook 6500, Appendix D establishes high-level policy and procedures for contingency planning and plan testing. Our audit identified the following deficiencies related to contingency planning:

- Many Information System Contingency Plans had not been updated to reflect lessons learned from contingency and disaster recovery tests, provide detailed recovery procedures for all system priority components, or reflect current operating conditions.
- Alternate processing site agreements between the regional offices and Information Technology Centers were not in place to ensure all parties are aware of respective responsibilities in the event of a disaster.
- Backup tapes for mission-critical systems were not encrypted prior to being sent offsite for storage.
- A significant data loss occurred at the Austin Information Technology Center due to inadequate backup and change management procedures.

Incomplete documentation of test plans, test results, and alternate processing site agreements prevent timely restoration of services in the event of system disruption or disaster. Inadequate backup testing leads to critical system failures. Inadequate communication of test results may also prevent lessons learned from being recognized and adopted. 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, updated plans continue to have weaknesses similar to those noted in FY 2012.

### Recommendations

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

18. 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. *(This is a repeat recommendation from last year.)*

19. We recommended the Executive in Charge for Information and Technology ensure that agreements for alternate processing sites have been established that define the roles and responsibilities for alternate locations in the event of a disaster. *(This is a repeat recommendation from last year.)*

20. We recommended the Executive in Charge for Information and Technology review change management procedures to ensure that any changes to system backup procedures are appropriately tested, validated, documented, and approved. *(This is a new recommendation.)*

## Finding 6 Incident Response

VA is unable to monitor all external interconnections and internal network segments for malicious traffic or unauthorized systems access attempts. 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. Audit teams identified deficiencies with VA's security incident management and external network monitoring processes.

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 has not fully implemented security information and event management technologies needed for effective event correlation analysis. VA does not have automated 24-hour security alert capability for all platforms and databases hosted at its Information Technology Centers. Furthermore, VA did not provide the OIG's Office of Audits and Evaluations with timely notifications of network intrusions and system compromises.

To improve incident management, VA's Network Security Operations Center 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, unknown and unmonitored connections still exist. In addition, our audit teams continued to identify several system interconnections without valid Interconnection Security Agreements and Memoranda of Understanding to govern them. Ineffective monitoring of external network interconnections could prevent VA from detecting and responding to intrusion attempts in a timely manner.

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. 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

21. We recommended the Executive in Charge for Information and Technology fully implement an automated 24-hour security event and incident correlation solution to monitor security for all systems interconnections, database security events, and mission-critical platforms supporting VA programs and operations. *(This is a repeat recommendation from last year.)*

22. We recommended the Executive in Charge for Information and Technology identify all external network interconnections and ensure appropriate Interconnection Security Agreements and Memoranda of Understanding are in place to govern them. *(This is a repeat recommendation from last year.)*

23. 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 last year.)*

24. We recommended the Executive in Charge for Information and Technology provide the Office of Inspector General with timely and formal notifications of network intrusions and system compromises in accordance with the Federal Information Security Management Act. *(This is a new recommendation.)*

## Finding 7 Continuous Monitoring

VA lacks an effective continuous monitoring process to identify unsecure system configurations and perform automated monitoring for unauthorized software and hardware devices. In addition, VA has not defined an inventory of authorized hardware and software nor implemented processes for removing unauthorized software on its systems. NIST Special Publication 800-53, Revision 3, *Recommended Security 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 operating system software, and inconsistent platform security standards across the enterprise. Without monitoring software and applications installed on VA devices, employees may introduce potentially dangerous software and malware into the VA computing environment.

To better meet continuous monitoring requirements, VA's Information Security Continuous Monitoring program's 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 DHS 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 the Information Security Continuous Monitoring program is to examine the enterprise to develop a real-time analysis of actionable risks that may adversely impact mission-critical systems.

VA has improved systems and data security control protections by implementing technological solutions, such as secure remote access, application filtering, and portable storage device encryption. Further, VA is deploying 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 can 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

25. 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 modified repeat recommendation from last year.)*

26. 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 modified repeat recommendation from last year.)*

## Finding 8 Security Capital Planning

VA has not implemented processes to fully account for security-related costs within its capital planning and investment control budget process. As a result, the audit team was unable to trace Plans of Action and Milestones (POA&Ms) remediation costs to corresponding Exhibit 300s for certain mission-critical systems. NIST Special Publication 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, states "the POA&M process provides a direct link to the capital planning process." On October 17, 2001, OMB issued Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, stating "for each POA&M that relates to a project (including systems) for which a capital asset plan and justification (exhibit 300) was submitted or was a part of the exhibit 53, the unique project identifier must be reflected on the POA&M."

In line with this Federal guidance, VA policy requires that security be included within the capital planning process. However, VA-specific guidance for integrating security into the budgeting process does not exist. Consequently, VA lacks procedures to ensure traceability of POA&M remediation costs to Exhibit 300s. For the future, guidance is needed to ensure security-related needs are consistently evaluated and integrated into the capital planning budget process in accordance with set standards. Without specific guidance, VA cannot ensure that information security is integrated throughout the system life cycle and adequate funding is budgeted to meet information security requirements.

### Recommendation

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. *(This is a repeat recommendation from last year.)*

## Finding 9 Contractor Systems Oversight

In FY 2013, 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 2013. Specifically:

- VA did not provide "Authorizations to Operate" for selected contractor-managed systems, formally acknowledging existing system security risks and security controls.
- VA did not provide evidence that contractor system security controls were appropriate.
- VA did not provide an annual inventory of contractor systems, including system interfaces and interconnection agreements.
- VA does not have adequate controls for monitoring cloud computing systems hosted by external contractors.

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

28. We recommended the Executive in Charge for Information and Technology implement procedures for overseeing contractor-managed, cloud-based systems, ensuring OIG access to those systems, and ensuring information security controls adequately protect VA sensitive systems and data. *(This is a modified repeat recommendation from last year.)*

29. 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 last year.)*

## Finding 10 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 by residents 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

30. 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 last year.)*

***Summary of Response From the Executive in Charge for Information Technology***

The Executive in Charge for Information and Technology generally concurred with the 30 findings and recommendations provided in the main body of this report and prepared a response, which is presented in Appendix D. In his comments, the Executive in Charge for Information and Technology stated that VA has implemented a Governance, Risk and Compliance tool as a major element of its agency-wide risk management governance program. This tool is intended to provide real-time monitoring of VA's system security posture as well as ensure that Plans of Action and Milestones are updated with current information. In general, management's comments and corrective action plans are responsive to the 30 recommendations. However, the responses to Recommendations 11 and 18 were not adequate as they did not provide clear corrective action plans and target completion dates.

Further, the Executive in Charge for Information and Technology stated that he intended to provide responses to the five prior-year recommendations in Appendix A after performing a review of ongoing corrective actions. Similar to responses provided over the past several years, management's approach to addressing these open prior-year recommendations is inadequate. 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 IT material weakness from this year's audit of VA's Consolidated Financial Statements. Following is our assessment of the status of VA's corrective actions to address each open prior-year recommendation in Appendix A:

- FY 2010–21: The status of corrective actions is unclear as VA did not describe actions taken to ensure risk assessments accurately reflect the current control environment.
- FY 2006–03: The status of corrective actions is unclear as VA did not describe the percentage of position descriptions that were updated in response to the recommendation.
- FY 2006–04: The status of corrective actions is unclear as VA did not describe the percentage of work completed to ensure that appropriate levels of background investigations are conducted for all VA employees and contractors.
- FY 2006–08: The status of corrective actions is unclear as VA did not describe the percentage of work completed to mitigate wireless security vulnerabilities and implement standard network configurations.
- FY 2006–09: The status of corrective actions is unclear as VA did not describe the percentage of work completed to eliminate or mitigate the use of clear text protocols across the enterprise.

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 2014.

# 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 2010–21 | We recommend 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.<br><br>**OIG comments:** The status of corrective actions is unclear as VA did not provide an adequate response to the open recommendation. The response needs to describe the actions taken to ensure risk assessments accurately reflect the current control environment. | In Progress | To Be Determined | VA is establishing a Risk Management Governance Board, which will implement uniform risk assessment procedures throughout VA.<br><br>Risk assessment exceptions continued to be identified during FISMA testing. |
| FY 2006–03 | We recommend 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.<br><br>**OIG comments:** The status of corrective actions is unclear as VA did not provide an adequate response for the open recommendation. The response needs to describe the percentage of position descriptions updated through FY 2013. | In Progress | To Be Determined | VA Directive and Handbook 0710, *Personnel Suitability and Security Program* documents have been updated.<br><br>VA developed action items to better coordinate reviews of existing position descriptions, position risk and sensitivity determinations, and current levels of employee background investigations. |

| Number | Recommendation | Status (In Progress or Closed) | Estimated Completion | Corrective Actions |
|---|---|---|---|---|
| FY 2006–04 | We recommend 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.<br><br>**OIG comments:** The status of corrective actions is unclear as VA did not provide an adequate response to the open recommendation. The response needs to describe the percentage of work completed to ensure that appropriate levels of background investigations are conducted for all VA employees and contractors. | In Progress | To Be Determined | VA established the Security Investigation Center to ensure background investigations are conducted.<br><br>The Office of Operations, Security, and Preparedness is coordinating actions to improve procedures for ensuring background investigations and reinvestigations are completed for all applicable VA employees and contractors in a timely manner.<br><br>Exceptions related to timely background investigations continued to be identified during FY 2013 FISMA testing. |

| Number | Recommendation | Status (In Progress or Closed) | Estimated Completion | Corrective Actions |
|---|---|---|---|---|
| FY 2006–08 | We recommend 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.<br><br>**OIG comments:** The status of corrective actions is unclear as VA did not provide an adequate response to the open recommendation. The response needs to describe the percentage of work completed to mitigate wireless security vulnerabilities and implement standard network configurations. | In Progress | To Be Determined | VA developed Directive 6512, *Secure Wireless Technology*, 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.<br><br>VA has begun replacing the legacy wireless networks with more robust and secure wireless networks, and defining strict configuration guidelines and implementation plans.<br><br>VA established the National Wireless Infrastructure Team to ensure all authorized VA wireless access points use a standard wireless network configuration.<br><br>Potential rogue access points continued to be identified during FY 2013 FISMA testing. |

| Number | Recommendation | Status (In Progress or Closed) | Estimated Completion | Corrective Actions |
|---|---|---|---|---|
| FY 2006–09 | We recommend the Assistant Secretary for Information and Technology identify and deploy solutions to encrypt sensitive data and resolve clear text protocol vulnerabilities.<br><br>**OIG comments:** The status of corrective actions is unclear as VA did not provide an adequate response to the open recommendation. The response needs to describe the percentage of work completed to eliminate or mitigate the use of clear text protocols across the enterprise. | In Progress | To Be Determined | VA is developing and integrating multiple technologies across the enterprise to encrypt sensitive data, both at rest and in transit. The technologies include:<br><br>• Deploy Sanctuary across the enterprise to ensure only authorized, encrypted, Universal Serial Bus devices are in use.<br><br>• Deploy laptop and desktop encryption.<br><br>• Deploy Data Transmission/ Attachmate to safely host information on the Web.<br><br>VA's "Visibility to Everything" (Server and Desktop) program verifies deployment of the above technologies and allows VA to remediate identified deficiencies.<br><br>Clear text protocol vulnerabilities continued to be identified during our FY 2013 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 memoranda 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 November 2013, OMB issued Memorandum M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. Federal agencies are to focus on implementing the Administration's three cybersecurity priorities established in FY 2012: (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 2013 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 feeds 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/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 2013. 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 teams' performance.

This year's work included evaluation of 79 selected major applications and general support systems hosted at 24 VA facilities to support Veterans Health Administration, Veterans Benefit Administration, and National Cemetery 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 2013 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— Cincinnati, OH
- Terremark, Cloud Service Provider—Culpepper, VA
- VA Medical Facility—Hampton Roads, VA
- Information Technology Center—Hines, IL
- VA Medical Facility—Kansas City, MO
- VA Medical Facility—Little Rock, AK
- VA Regional Office—Little Rock, AK
- VA Medical Facility—Manchester, NH
- Network and Security Operations Center—Martinsburg, WV

- Capitol Regional Readiness Center—Martinsburg, WV
- VA Medical Facility— Miami, FL
- VA Medical Facility—New Orleans, LA
- VA Regional Office—New Orleans, LA
- VA Medical Facility—Oklahoma City, OK
- Information Technology Center—Philadelphia, PA
- VA Insurance Center—Philadelphia, PA
- VA Regional Office—Philadelphia, PA
- Loan Guaranty Contractor Managed Facility—Plano, TX
- National Cemetery Administration—Quantico, VA
- VA Medical Facility—Reno, NV
- VA Medical Facility— San Antonio, TX
- VA Medical Facility— San Francisco, CA
- 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 18, 2014

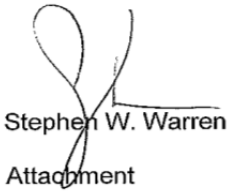
**From:** Executive in Charge and Chief Information Officer, Office of Information and Technology (005)

**Subj:** Draft Audit Report: Federal Information Security Management Act (FISMA) Assessment for FY 2013

**To:** Assistant Inspector General for Audits and Evaluations (52CT)

Thank you for the opportunity to review the subject draft audit report. The Office of Information and Technology concurs and submits the attached detailed comments and a partial set of artifacts to the report's 30 recommendations.

Remaining artifacts will be provided under separate cover. We appreciate your time and attention to our information security program. If you have any questions, contact me at 202-461-6910, or have a member of your staff contact Martha Orr, Executive Director for Quality, Performance and Oversight, at 202-461-6910.



Stephen W. Warren

Attachment

Attachment

**Office of Information and Technology**
**Comments to Draft OIG Report,**
**"Federal Information Security Management Act Audit for FY 2013"**
**OIG Recommendations and OIT Responses:**

**Recommendation 1:** We recommend the Executive in Charge for Information and Technology fully develop 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 last year.)

**OIT Response:** Concur. The Office of Information and Technology (OI&T) has implemented the Governance, Risk and Compliance (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 The tool is used in concert with existing IT monitoring and tracking tools, such as IBM End-Point Manager (IEM), SolarWinds, 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 Authority to Operate (ATO) decisions.

OI&T maintains a mature Enterprise Risk Management (ERM) organization that proactively manages risks that are applicable to the OIT 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 OIT enterprise risks. This past year, the Continuous Readiness and Information Security Protection (CRISP) Governance Council was chartered and implemented. This Governance Council, comprised of membership from all Department stakeholders such as VHA, VBA and NCA, is fully sanctioned by VA leadership to ensure all VA organizations are responsive to initiatives and actions necessary to maintain heightened awareness of information security and protection and to identify, monitor and manage risk across the enterprise.

Completed: Recommend Closure

**Recommendation 2:** We recommend the Executive in Charge for Information and Technology implement mechanisms to ensure sufficient supporting documentation is captured in the central database to justify closure of Plans of Action and Milestones. (This is a repeat recommendation from last year.)

**OIT Response:** Concur. The GRC tool, implemented at the end of FY 2013, monitors the real-time security posture of the VA's IT systems, and is the mechanism used to track active Plans of Action and Milestones (POA&M). VA transitioned active POA&M's from the SMART system to the GRC Risk Vision tool, leaving completed POA&M's in the SMART for historical purposes. The GRC tool is the sole repository for all supporting artifacts to document POA&M process and maintains documentation to justify closure of POA&M's. Additionally, mechanisms, such as compliance reviews by OCS staff, annual self-assessments by facility staff, and control implementation validation by Information Security Officers (ISO) are currently in place to randomly check POA&M documentation

Complete – Recommend Closure

**Recommendation 3:** We recommend the Executive in Charge for Information and Technology define and implement clear roles and responsibilities for developing, maintaining, completing, and reporting Plans of Action and Milestones. (This is a repeat recommendation from last year.)

**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. VA Handbook 6500 includes, in section four, "Information Security Responsibilities," the responsibilities regarding POA&Ms for the Deputy CIO for SDE/System Owners, Executive Director for Quality, Performance and Oversight, Under Secretaries, Assistant Secretaries, and Other Key Officials, Program Directors/Facility Directors, ISOs, Local Program Management, Local CIOs/System Administrators/Network Administrators/Database Managers, CO/COR, and Local HR Staff/Security and Law Enforcement Staff. POA&M responsibilities are also addressed in VA Handbook 6500, Appendix F under controls CA-5: Plan of Action and Milestones and PM-4: Plan of Action and Milestones.

VA Handbook 6500.3 includes, in section three, "Responsibilities," the roles and responsibilities regarding POA&Ms for the VA CIO, DAS OIS, 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 GRC Risk Vision tool, implemented in August 2013, is actively used to provide an automated method for assigning POA&M management roles and responsibilities to system owners, information security officers, administrators, and mangers.

Complete – Recommend Closure

**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 POA&M's are updated with currently status information. These mechanisms are inherent in the work flow of the tool and provide the necessary checks and balances to ensure information can be entered accurately. Integral to the specially designed workflows of RiskVision is a two-step validation process. The information security control provider is required to provide evidence of the control implementation status. The assigned Information Security Officer (ISO) is required to validate the implementation status. If found deficient, the ISO generates a finding. Additionally, with the IBM Endpoint Manager (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. This tool is the sole repository of all active POA&M's and is actively used to manage the POA&M process.

Completed – Recommend Closure

**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 and ownership information. (This is a 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 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. Additionally, the requirement to have accurate, comprehensive and up-to-date system security plans is required by VA policy, as discussed in VA Handbook 6500.

Complete – Recommend Closure

**Recommendation 6:** We recommend the Executive in Charge for Information and Technology implement improved processes for updating key security documents such as risk assessments, security impact analyses, and security self-assessments on at least an annual basis and ensure all required information accurately reflects the current environment and new risks in accordance with Federal standards. (This is a new recommendation.)

**OIT Response:** Concur. With the implementation of the GRC tool in August 2013, a new, improved process was developed and established for all IT system risk assessments. Based on actual findings, which flows through the automated system, we are now continuously monitoring and managing risk assessments, giving 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, updates are accomplished throughout the year, and analysis of the data ensure remediation activities are appropriate to the current environment.

Complete – Recommend Closure

**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. VA implemented a process last year 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) and Standard Operating Procedures (SOP) are in place to ensure a structured, repeatable process. OIT continues to update information system user and system account management policy guidance and processes that will emphasize requirements for system owners, systems administrators, and security staffs to regularly review the account privileges and access levels for all system users on at least an annual basis. This review will be re-emphasized as an item that must be covered during the annual testing of application security controls.

Complete – Recommend Closure

**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 OIT 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. At each facility, the local Information Security Officer (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 separated users from VA occurs every 90 days. Also part of the OIT Security Calendar process, this review ensures that staff, contractors and volunteers no longer with VA have access privileges removed from e-mail, administrator rights and other VA systems. Please see attached artifacts.

Completed – Recommend Closure

**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. Implementation is currently unfunded in terms of storage and staffing within the medical center/field operation environment. These tools have been implemented in our Data Center and by our Network and Security Operations Center. Early installation of the devices for our field locations is contingent on funding in FY 2014. If we are unsuccessful in obtaining FY 2014 funding, this requirement will be incorporated in the FY 2015 budget operating plan.

Target Completion Date: September 30, 2015 (contingent upon receipt of funds)

**Recommendation 10:** 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. Except for a limited number of VHA clinical users, mechanisms have been implemented to ensure all remote access computers have updated security patches and antivirus. OI&T is working with VHA to verify key performance criteria for the critical work flows. That analysis will be completed by the end of this fiscal year, followed by implementation.

Target Completion Date: April 30, 2015

**Recommendation 11:** We recommend the Executive in Charge for Information and Technology implement two-factor authentication for remote access throughout the agency. (This is a repeat recommendation from last year.)

**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 process have been developed that accommodate the use of PIV cards by VHA. Implementation continues throughout the rest of the Department.

Target Completion Date: To Be Determined – Dependent on implementation of new work processes by VHA

**OIG comments:** The status of corrective actions is unclear as VA did not provide a concrete corrective action plan or clear target completion date.

**Recommendation 12:** We recommend the Executive in Charge for Information and Technology develop and implement policies and procedures for restricting privileged remote access from foreign countries that may pose a significant security risk to VA systems. (This is a new recommendation.)

**OIT Response:** Concur. The DAS for OIS signed a memo (attached) on January 15, 2014 prohibiting access to VA's network from non-NATO countries, with the exception of countries where VA has approved operations established (e.g., Philippines, South Korea). This requirement has been formalized in the current draft version of VA Handbook 6500, which will be published by the end of fiscal year 2014. Additionally, OIS has begun blocking Top Level Domains for country codes and IP addresses for those countries noted above.

Completed - Recommend Closure

**Recommendation 13:** We recommend the Executive in Charge for Information and Technology implement effective automated mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and Web application servers. (This is a repeat recommendation from last year.)

**OIT Response:** Concur. VA has implemented an enterprise-wide vulnerability management program that makes use of a number of scanning tools to identify security deficiencies. The outputs from the

scanning tools are then 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. VA will continue to enhance the vulnerability management program by making use of the security and information event management (SIEM) technology, which currently is in place at the Enterprise Operations (EO) data centers. The SIEM solution will collect audit logs and alerts and facilitate the continuous identification of vulnerabilities that require priority corrective actions. The next steps in the expanded implementation of SIEM have been defined as consisting of three phases: EO Data Centers (complete), Gateways and Network Backbone and the NSOC (concurrently schedule to be awarded by 30 April 2014) and Regional Data Centers Systems (currently in planning to identify requirements and funding levels).

Target Completion Date – Phase Two (September 30, 2014)/Phase Three (September 30. 2015).

**Recommendation 14:** We recommend the Executive in Charge for Information and Technology implement a 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. 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 received 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.

Completed – Recommend Closure

**Recommendation 15:** We recommend the Executive in Charge for Information and Technology implement standard security configuration baselines for all VA operating systems, databases, applications, and network devices. (This is a 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 for printers, thin clients, and SQL databases, including a plan to begin implementation in FY2014

Target Completion Date – December 31, 2015

**Recommendation 16:** We recommend the Executive in Charge for Information and Technology implement procedures to enforce a system development and change control framework that integrates information security throughout the life cycle of each system. (This is a repeat recommendation from last year.)

**OIT Response:** Concur. In 2009 OIT Product Development (PD) and OIT Service Delivery 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 a necessary project team member 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 the Office of Information Security 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.

Target Completion Date: September 30, 2015

**Recommendation 17:** We recommend the Executive in Charge for Information and Technology implement processes to ensure information system contingency plans are updated with the required information and lessons learned are communicated to senior management. (This is a repeat recommendation from last year.)

**OIT Response:** Concur. 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 reports the compliance status of VA systems with the guidance. These compliance reports will be forwarded to the executive level to ensure proper follow-up. All offices with systems not in compliance with the guidance will need to apply resources to update their contingency plans, and test them. OIS Office of Business Continuity will work with all non-compliant systems to provide support and assistance. Projected completion date for all non-compliant VA system contingency plans to be brought into compliance is March 31, 2015

Target Completion Date: March 31, 2015

**Recommendation 18:** 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 new recommendation.)

**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.

Target Completion Date – High level program plan – October 31, 2014, completion for remaining tasks to be determined once the high level program plan is completed.

**OIG comments:** The status of corrective actions is unclear as VA did not provide a clear target completion date for subordinate tasks.

**Recommendation 19:** We recommend the Executive in Charge for Information and Technology ensure that agreements for alternate processing sites have been established that define the roles and responsibilities for alternate locations in the event of a disaster. (This is a new recommendation.)

**OIT Response:** Concur. Region level alternate processing site agreements and MOU's have been developed that define the roles and responsibilities for alternate locations in the event of a disaster. These agreements have been provided to the field CIO's and were implemented.

Complete – Recommend Closure

**Recommendation 20:** We recommend the Executive in Charge for Information and Technology review change management procedures to ensure that any changes to system procedures are appropriately tested, validated, documented and approved. (This is a repeat recommendation from last year.)

**OIT Response:** Concur. OI&T will review change management procedures to ensure that any changes to system procedures are appropriately tested, validated, documented and approved.

Target Completion date – December 31, 2014

**Recommendation 21:** We recommend the Executive in Charge for Information and Technology fully implement an automated 24-hour security event and incident correlation solution to monitor security for all systems interconnections, database security events, and mission-critical platforms supporting VA programs and operations. (This is a repeat recommendation from last year.)

**OIT Response:** Concur. Security Information & Event Management (SIEM) Procurement by the NSOC is scheduled for FY14. Progress was delayed since our Request for Proposal (RFP) did not yield qualified vendors and we have had to repeat the RFP process.

Target Completion Date: December 31, 2014

**Recommendation 22:** We recommend the Executive in Charge for Information and Technology identify all external network interconnections and ensure appropriate Interconnection Security Agreements and Memoranda of Understanding are in place to govern them. (This is a repeat recommendation from last year.)

**OIT Response:** Concur. All Memoranda of Understanding (MOU) and Interconnection Security Agreements (ISA) for known external network connections have been reviewed (as part of OIT's annual review) and updated to reflect operational environments. This review process is now part of an annual cycle. OIT has documented these known connections and has also published guidance on this subject.

Complete – Recommend Closure

**Recommendation 23:** 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 VA Network Security Operations Center (VA-NSOC) initiated an Incident Response (IR) Working Group to review current cyber security incident response policies, procedures and performance measures. The working group will be providing 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 VA-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 working group will also establish performance metrics to measure effectiveness of the incident response activities, and has already worked to incorporate new metrics into the May 2014 OIT MPR. The target implementation date for additional VA policy revision and performance metrics is 30 September 2014. The working group will also establish performance metrics to measure effectiveness of the incident response activities, and has already worked to incorporate new metrics into the May 2014 OIT Performance Review (PR).

The target date for revising VA's Incident Response Plan to include new performance metrics is 30 September 2014. OIT and the VA-NSOC participated and tested incident response capabilities during the VA National Level Exercise in July 2012. The Incident Response Working Group will continue to review

past cyber security incident response testing and recommend testing the incident response capability on an annual basis. VA will also coordinate with the Department of Homeland Security to participate in other upcoming cyber incident response exercises that may be planned by the United States Computer Emergency Response Team. The target date for testing the department's incident response capability is 31 December 2014. The VA-NSOC worked with the IT Workforce Development office during 2012 and 2013 to develop the NSOC Cyber Security Competency Model in the VA Talent Management System (TMS). The competency model is currently used by all VA-NSOC personnel. All supervisors are also required to complete supervisory training in TMS, as well as attend an on-site week of training in the core competencies of supervision in the VA and federal service. OIT will ensure that role based security incident response training is included in the Individual Development Plans, and completed by the appropriate incident response personnel.

Target Completion Date – December 31. 2014

**Recommendation 24:** We recommend the Executive in Charge for Information and Technology provide the OIG with timely and formal notifications of network intrusions and system compromises in accordance with FISMA. (This is a new recommendation.)

**OIT Response:** Concur. We are currently providing OIG with timely and formal notification of network intrusions and system compromises in accordance with FISMA. This is accomplished via automatic notification in Remedy to OIG's Computer Crimes division. Our Standard Operating Procedure and a sample of transmissions is attached.

Complete – Recommend Closure

**Recommendation 25:** 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. Implementation on this recommendation continues. VA has a white list for approved software and a black for unauthorized software. VA has a process for requesting adding software for the white list. Implementation for continuous monitoring to prevent use of unauthorized is still underway.

Target Completion Date: September 30, 2014

**Recommendation 26:** 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 modified repeat recommendation from last year.)

**OIT Response:** Concur. VA has a white list for approved software and a black list for unauthorized software. VA has several tools such as Tivoli Endpoint Manager, Microsoft's System Center Configuration Manager and Orion, which when fully deployed will identify major and minor software applications.

Complete – Recommend Closure

**Recommendation 27:** We recommend the Acting Assistant Secretary for Information and Technology develop 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. (This is a repeat recommendation from last year.)

**OIT Response:** Concur. Office of Information Technology (OIT) will develop procedures that require Plans of Action and Milestones (POA&Ms) to be formally included in OIT's Planning, Programming, Budgeting, and Execution Process (PPBE). The PPBE process will provide 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). Subsequent to the policy statement, a process will be developed and issued instructing POA&M developers how to enter their material into the PPBE process for programmatic and funding consideration. These two steps will provide funding traceability from POA&M through PPBE and into CPIC (Exhibit 300s).

Target Completion Date: June 30, 2014

**Recommendation 28:** We recommend the Executive in Charge for Information and Technology implement procedures for overseeing contractor-managed cloud-based systems, ensuring OIG access to those 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 (Phase 1), where appropriate, the Technical Acquisition Center (TAC) is incorporating 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, to fully cooperate with all audits, inspections, investigations, or other reviews conducted by or on behalf of the Contracting Officer or the agency Office of Inspector General and to provide the Contracting Officer, designated representative of the Contracting Officer, and representatives of the agency's Office of Inspector General, full and free access to the Contractor's (and Subcontractors') facilities, installations, operations documentation, databases, and personnel used for contract hosting services.

The long term solution (Phase 2) specific to contractor-managed cloud-based systems, the "Cloud Computing" related clauses developed are required to go through formal rulemaking. They cannot be considered as either a modification to, nor an Alternate of an existing FAR clause (FAR 52.215-2 – Audit and Records—Negotiation (OCT 2010)). Note that "modifications" are considered minor changes and an "Alternate" to a given provision or clause is prescribed in the FAR subject text where Alternates are prescribed. The clause language does not fit under either definition. FAR 52.215-2 is an existing FAR clause. 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.

Target Completion Date: Phase 1 – October 1, 2014, Phase 2 – TBD, Based on time for Rulemaking

**Recommendation 29:** 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. The VA is continuing to improve efforts towards obtaining the highest degree possible of accuracy of its FISMA systems. At present, IBM Endpoint Manager is present on 95% of the Department's servers and desktops. Further, Solarwinds is on an equivalent percentage of the network devices. Excluded systems and devices defined as "other" are being reviewed to determine the appropriate steps required to complete the inventory. The system inventory, maintained by GRC, is reviewed continuously by the Risk Vision Working Group and by OIS management. Completed annual review and are moving to a monthly validation of systems in the inventory to ensure they are assigned to the proper accreditation boundary.

Target Completion Date: Completed.

**Recommendation 30:** 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 continues to excel in the area of security awareness training, reporting that more than 98% of VA staff and contractors take updated security awareness training annually. Compliance to this training requirement is constantly monitored throughout the year and training stand downs occur for all organizations within VA each March. 100% of users should have completed security awareness training before access is granted. VA policy as stated in 6500 is to not grant access until security awareness training is completed. IT Workforce Development can run TMS reports to verify if a person has completed the training but has no way to determine when access was granted. The local ISO authorizes network access. Office of Information Technology (OIT) will continue to work with the various VA entities specifically identified in this report to ensure the completion of #10176 VA Privacy and Information Security Awareness and Rules of Behavior in the VA's Talent Management System (TMS). This training is the Inspector General's (IG's) accepted training process currently developed each year by the mandatory training business owner, OIT's IT Workforce Development team. VA's most current compliance rate is attached.

Target Completion Date: Completed.

# 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<br>Carol Buzolich<br>Elijah Chapman<br>Michael Miller<br>Neil Packard<br>Richard Purifoy<br>Felita Traynham |

# 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.**