VA Office of Inspector General

OFFICE OF AUDITS & EVALUATIONS

Department of Veterans Affairs

Federal Information Security Management Act Audit for Fiscal Year 2012

June 27, 2013
12-01712-229

ACRONYMS AND ABBREVIATIONS

CRISP	Continuous Readiness in Information Security Program
DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones

Department of Veterans Affairs

Memorandum

Date: June 18, 2013

From: Assistant Inspector General for Audits and Evaluations

Subj: Final Report: *VA's Federal Information Security Management Act Audit for FY 2012*

To: Acting Assistant Secretary for Information and Technology

1. Enclosed is the final audit report, *Federal Information Security Management Act Audit for FY 2012*. The Office of Inspector General (OIG) contracted with the independent public accounting firm, CliftonLarsonAllen LLP, to assess the Department of Veterans Affairs' (referred to herein as the Department) 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 annually review the agency's information security program and report the results to the Department of Homeland Security (DHS). DHS uses this data to assist in its oversight responsibilities and to prepare an annual report to Congress on agency compliance with FISMA.

3. The Department 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, the Department needs to focus on several key areas including:

   - Addressing security-related issues that contributed to the information technology material weakness reported in the FY 2012 audit of the Department's consolidated financial statements, including expediting implementation plans for corrective actions needed to effectively address the recommendations made in this report.
   - Successfully remediating high-risk system security issues in its Plans of Action and Milestones, and use that process to improve VA's information security posture.
   - Establishing effective processes for evaluating information security controls via continuous monitoring and vulnerability assessments.

4. CliftonLarsonAllen LLP was contracted to perform the FISMA audit and is responsible for the findings and recommendations included in the attached draft report dated June 2013. The OIG does not express an opinion on the effectiveness of the Department's internal controls during FY 2012.

5. This report provides 32 recommendations for improving VA's information security program; 27 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. During FY 2012, two recommendations were administratively closed because VA's corrective actions successfully addressed the underlying risks; a third recommendation was closed because it was superseded by a more current recommendation. Some recommendations have been modified to reflect new security risks identified during this year's audit.

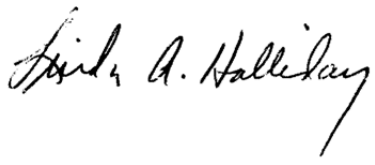
6. As part of this year's audit, CliftonLarsonAllen LLP examined whether the Department's corrective actions successfully addressed the outstanding recommendations. Some recommendations were not closed because relevant information security policies and procedures were not finalized or information security control deficiencies were repeated or newly identified during the FY 2012 FISMA audit.

7. We remain concerned that the presented implementation plan in your official comments, contains milestones for completion well into FY 2014, for the following areas:

   - Agency-wide risk management program (recommendation 5)
   - Identity management and access control (recommendations 7, 9, and 10)
   - Configuration management controls (recommendation 12)
   - System development / change management controls (recommendation 15)
   - Incident response (recommendation 19)
   - Continuous network monitoring (recommendation 22)

8. The impact of these open recommendations needs to be considered in the FY 2013 assessment of VA's security posture. Since several recommendations will remain open through FY 2014, the delays implementing effective corrective actions can potentially contribute to reporting an IT material weakness in this year's audit of VA's Consolidated Financial Statements.

9. Our independent auditors will follow up on the outstanding recommendations and evaluate the adequacy of corrective actions during the FY 2013 FISMA audit. However, in an effort to better oversee the implementation plan to completion in FY 2014, OIG will require interim progress reports quarterly starting October 1, 2013.



LINDA A. HALLIDAY

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

May 30, 2013

The Honorable George Opfer
Inspector General
Department of Veterans Affairs
801 I Street, Northwest
Washington, DC 20001

Dear Mr. Opfer:

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, 2012 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 2012 through November 2012. 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.

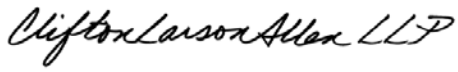
We performed limited reviews of the findings, conclusions, and opinions expressed in this report that were related to the financial statement audit performed by CliftonLarsonAllen LLP. The financial statement audit results have been combined with the FISMA performance audit findings. We do not provide 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 2012. 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 FISMA Audit for FY 2012

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 2012 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 an 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. Also, prior FISMA recommendations remain open.

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 4,000 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 2012 consolidated financial statement audit, CliftonLarsonAllen LLP concluded a material weakness still exists in VA's information security program.

What We Recommend

We recommend the Acting Assistant Secretary for Information and Technology implement comprehensive measures to mitigate security vulnerabilities affecting VA's mission-critical systems.

Agency Comments

The Acting Assistant Secretary for Information and Technology agreed with our findings and recommendations and provided plans for corrective actions.

OIG Comments

We will monitor implementation of the action plans. However, we remain concerned that several of the action plans are not expected to be in place until September 2014 for both new and prior recommendations. OIG will monitor implementation through interim progress reports until proposed actions are complete.

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 FY 2012 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 the Department's information security program through inquiries, observations, and tests of selected controls supporting 81 major applications and general support systems at 22 VA facilities. 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 32 total recommendations, including four new recommendations, for improving VA's information security program. 27 recommendations are included in the report body and five recommendations are provided in Appendix A. The Appendix addresses the status of recommendations not included in the report body and VA's plans for corrective action. During FY 2012, two recommendations were administratively closed because VA's corrective actions successfully addressed the underlying risks; a third recommendation was closed because it was superseded by a more current recommendation. These recommendations are annotated as "closed" in Appendix A. The FY 2011 report provided 31 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, the Department 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 began updating VA Handbook 6500 to be consistent with revised NIST Special Publications and to supplement existing VA directives and handbooks. OMB Memorandum M-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* issued in September 2012, 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). 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:

- Training, both role-based and security awareness
- Testing contingency plans
- Reducing the number of outstanding Plans of Action and Milestones (POA&Ms)
- Developing initial baseline configurations

- Reducing the number of individuals with outdated background investigations
- Improving data center Web application security

Because the CRISP initiative was not launched until March 2012, the process improvements were not implemented for an entire fiscal year.

Moving forward, VA needs to ensure a proven process is in place to sustain the improvements achieved thus far. VA also needs to continue to address control deficiencies existing 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 approach, POA&Ms, and system security plans, which are discussed in the following section. Each of these processes is critical for protecting the Department'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. Specifically, 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 began updating 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 and strategy 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 reduced the number of open POA&Ms from approximately 15,000 in FY 2011 to

4,000 in FY 2012. POA&Ms identify which actions must be taken to remediate system security risks and improve VA's information security posture. POA&M reductions partially resulted from VA leveraging FISMA stakeholder teams to ensure that corrective actions address previous FISMA report recommendations.

VA has made progress in updating and closing POA&Ms in a timelier 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 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 input 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. Further, without sufficient documentation in the central database to justify closure of POA&Ms, VA cannot ensure that corresponding security risks have been fully mitigated.

System Security Plans

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 recommend the Acting Assistant Secretary 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 recommend the Acting Assistant Secretary 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 recommend the Acting Assistant Secretary 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 recommend the Acting Assistant Secretary for Information and Technology implement mechanisms to ensure Plans of Action and Milestones are updated to accurately reflect current status information. *(This is a repeat recommendation from last year.)*

5. We recommend the Acting Assistant Secretary 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 recommend the Acting Assistant Secretary 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.)*

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, 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 application privileges within major applications. This occurred because VA has not implemented effective reviews to eliminate such 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. Such audit trail reviews are critical to facilitate 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. In addition, multi-factor authentication for remote access has not been 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 before connecting to VA networks.

Recommendations

7. We recommend the Acting Assistant Secretary for Information and Technology implement mechanisms to enforce VA password policies and standards on all operating systems, databases, applications, and network devices. *(This is a repeat recommendation from last year.)*

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

9. We recommend the Acting Assistant Secretary for Information and Technology enable system audit logs and conduct centralized

reviews of security violations on mission-critical systems. *(This is a repeat recommendation from last year.)*

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

11. We recommend the Acting Assistant Secretary for Information and Technology implement two-factor authentication for remote access throughout the agency. *(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

Assessments of Web-based applications identified several instances of VA data facilities hosting unsecure Web-based services that could allow malicious users to gain unauthorized access to VA information systems. Additionally, an attacker could potentially alter sensitive data or covertly run unauthorized programs on Web applications. NIST Special Publication 800-44, Version 2, *Guidelines in 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 assessments continue to identify a significant number of unsecure configuration settings that could allow any database user to gain unauthorized access to critical system information. NIST Special Publication 800-64, Revision 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 assessments again identified a significant number of outdated operating systems and vulnerable third-party applications that could allow unauthorized access to mission-critical systems and data. NIST Special Publication 800-40, 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 the Department'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 was still working to develop 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 and Federal Desktop Core Configurations were not consistently implemented on all VA systems. For example, testing at VA facilities revealed varying levels of compliance (88 to 96 percent) with Federal Desktop Core Configurations 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

12. We recommend the Acting Assistant Secretary 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 modified repeat recommendation from last year.)*

13. We recommend the Acting Assistant Secretary 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.)*

14. We recommend the Acting Assistant Secretary 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 its mission-critical systems. 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.

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. 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

15. We recommend the Acting Assistant Secretary 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 2011 audit. However, VA contingency plans still were not fully documented and test results were not consistently communicated to senior management. While VA Handbook 6500, Appendix D establishes high-level policy and procedures for contingency planning and plan testing, our assessment 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 Office 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.

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 testing may lead to critical system failures during the execution of system contingency plans. Inadequate communication of test results may 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.

Recommendations

16. We recommend the Acting Assistant Secretary 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 modified repeat recommendation from last year.)*

17. We recommend the Acting Assistant Secretary 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.)*

18. We recommend the Acting Assistant Secretary 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.)*

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 is the process of tying 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 also has no automated 24-hour security alert capability for all platforms and databases hosted at its Information Technology Centers.

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 an intrusion attempt in a timely manner.

Our audits continue 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 in a timely manner. 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

19. We recommend the Acting Assistant Secretary 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 modified repeat recommendation from last year.)

20. We recommend the Acting Assistant Secretary 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.)*

21. We recommend the Acting Assistant Secretary for Information and Technology implement more effective agency-wide incident response procedures to ensure timely resolution of computer security incidents in accordance with VA set standards. *(This is a modified repeat recommendation.)*

Finding 7 Continuous Monitoring

VA lacks an effective continuous monitoring process to identify its hardware and software inventory and perform automated monitoring for unauthorized software and hardware devices. 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 and vulnerable third-party applications and operating system software, and inconsistent platform security standards across the enterprise.

To better meet continuous monitoring requirements, VA's *Information Security Continuous Monitoring* Concept of Operations established a centralized, enterprise information technology framework that supports operational security demands for protection of critical information. VA's *Information Security Continuous Monitoring* process is being developed by the Office of Information and Technology's Office of Cyber Security. This framework is based on guidance from Continuous Monitoring Workgroup activities sponsored by the Department of Homeland Security and the Department of State. The goal of *Information Security Continuous Monitoring* 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 reveals that VA facilities have not made effective use of these tools to actively monitor their networks for unauthorized software, hardware devices, and system configurations.

Recommendations

22. We recommend the Acting Assistant Secretary for Information and Technology implement effective continuous monitoring processes to identify and prevent the use of unauthorized application software, hardware (including personal storage devices), and system configurations on its networks. *(This is a repeat recommendation from last year.)*

23. We recommend the Acting Assistant Secretary for Information and Technology develop a comprehensive software inventory process to identify major and minor software applications used to support VA programs and operations. *(This is a repeat recommendation from 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, formalized 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

24. 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.)*

Finding 9 Contractor Systems Oversight

In FY 2012, 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 2012. Specifically:

- VA did not provide "Authorizations to Operate" for selected contractor-owned and operated systems.
- 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.

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

Recommendations

25. We recommend the Acting Assistant Secretary for Information and Technology implement procedures for overseeing contractor-managed systems and ensuring information security controls adequately protect VA sensitive systems and data. *(This is a repeat recommendation from last year.)*
26. We recommend the Acting Assistant Secretary for Information and Technology implement mechanisms for updating the Federal Information Security Management Act systems inventory, including interfaces with contractor-managed systems, and annually review the systems inventory for accuracy. *(This is a repeat recommendation from last year.)*

Finding 10 Security Awareness Training

We noted improvements as part of the CRISP initiative 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 the Department'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

27. We recommend the Acting Assistant Secretary 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 modified repeat recommendation from last year.)*

Summary of Response from the Acting Assistant Secretary for Information Technology

The Department concurred with all findings and recommendations and prepared a response, which is presented in Appendix D. The Acting Assistant Secretary for Information and Technology stated that VA treats the protection of Veteran data very seriously. Accordingly, VA has embarked on a cultural transformation with implementation of the Continuous Readiness in Information Security Program (CRISP). The Acting Assistant Secretary stated that CRISP is a new operating model for protecting Veteran private and sensitive information. The program embodies an integrated approach to protecting sensitive information from inappropriate exposure or loss. Management's comments and corrective action plans are generally responsive to the recommendations. Recommendations will not close until relevant information security policies/procedures are finalized and information security control deficiencies are fully remediated. We will continue to evaluate VA's progress during our audit of the Department's information security program in FY 2013.

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. During FY 2012, two recommendations were administratively closed because VA's corrective actions successfully addressed the underlying risks; one recommendation was closed because it was superseded by a more current recommendation. 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 2011–02	We recommend the Assistant Secretary for Information and Technology dedicate resources to remediate the large number of unresolved Plans of Action and Milestones in the near term while concurrently focusing on addressing high-risk system security deficiencies.	Closed	Not Applicable	No exceptions were identified during FY 2012 FISMA testing.
FY 2011–22	We recommend the Assistant Secretary for Information and Technology identify and ensure personnel with specialized security responsibilities fulfill annual specialized computer security training requirements.	Closed	Not Applicable	No exceptions were identified during FY 2012 FISMA testing.
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.	In Progress	September 2013	VA is establishing a Risk Management Governance Board, which will implement uniform risk assessment procedures throughout VA.

Table. Status of Prior Year Recommendations

Number	Recommendation	Status (In Progress or Closed)	Estimated Completion	Corrective Actions
FY 2006–03	We recommend the Assistant Secretary for Information and Technology review and update all applicable position descriptions to better describe sensitivity ratings and better document employee personnel records and contractor files, including "Rules of Behavior" instructions, annual privacy and Health Insurance Portability and Accountability Act of 1996 training certifications, and position sensitivity level designations.	In Progress	To Be Determined	VA Directive and Handbook 0710, *Personnel Suitability and Security Program* documents have been updated. VA developed action items (March 2012) to better coordinate reviews of existing position descriptions, position risk and sensitivity determinations, and current levels of employee background investigations. This process will help ensure consistent application of VA Directive 0710, *Personnel Suitability and Security Program.*

Table. Status of Prior Year Recommendations

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.	In Progress	To Be Determined	VA established the Security Investigation Center to ensure background investigations are conducted. 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. Exceptions related to timely background investigations continued to be identified during FY 2012 FISMA testing.

Table. Status of Prior Year Recommendations

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 an effective and up-to-date methodology to protect against the interception of wireless signals and unauthorized access to the network and ensure the wireless network is segmented and protected from the wired network.	In Progress	To Be Determined	VA developed Directive 6512, *Secure Wireless Technology and Wireless Security*, to supplement VA Handbook 6500. The Directive provides guidelines for protecting VA wireless networks from signal interception, enhancing network security, and segmenting VA's wireless network from the wired network. VA has begun replacing the legacy wireless networks with more robust and secure wireless networks, defining strict configuration guidelines and implementation plans. VA has established the National Wireless Infrastructure Team to ensure all authorized VA wireless access points use a standard wireless network configuration. Potential rogue access points continued to be identified during FY 2012 FISMA testing.

Table. Status of Prior Year Recommendations

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.	In Progress	September 2013	VA is developing and integrating multiple technologies across the enterprise to encrypt sensitive data, both at rest and in transit. The technologies include: • Deploy Sanctuary across the enterprise to ensure only authorized, encrypted Universal Serial Bus devices are in use. • Deploy laptop and desktop encryption. • Deploy Data Transmission/ Attachmate to safely host information on the Web. VA's "Visibility to Everything" (Server and Desktop) program verifies deployment of the above technologies and allows the Department to remediate identified deficiencies. Clear text protocol vulnerabilities continued to be identified during our FY 2012 FISMA testing.
FY 2006–13	We recommend the Assistant Secretary for Information and Technology complete the implementation of two-factor authentication in accordance with NIST Special Publication 800-53.	Closed Superceded by recommendation FY 2012–11.	Not Applicable	

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. FISMA 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 the 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 Generals for preparing annual FISMA reports. In September 2012, OMB issued Memorandum M-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Managemen*t. 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 2012 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 will 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 2012. The OIG provided oversight of the contractor's performance.

Appendix C Scope and Methodology

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

This year's work included evaluation of 81 selected major applications and general support systems hosted at 22 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 2012 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—Birmingham, AL
- VA Medical Facility—Chillicothe, OH
- VA Medical Facility—Columbia, SC
- Capitol Region Data Center—Falling Waters, WV
- Information Technology Center—Hines, IL
- VA Medical Facility—Lexington, KY
- VA Medical Facility—Loma Linda, CA
- Capitol Regional Readiness Center—Martinsburg, WV
- VA Medical Facility—Memphis, TN

- Information Technology Center—Philadelphia, PA
- VA Insurance Center—Philadelphia, PA
- VA Regional Office—Philadelphia, PA
- Bank of America Contractor-Managed Facility—Plano, TX
- National Cemetery Administration—Quantico, VA
- VA Medical Facility—Salt Lake City, UT
- VA Regional Office—Salt Lake City, UT
- VA Central Office—Washington, DC
- VA Medical Facility—Washington, DC
- National Capital Region Benefits Office—Washington, DC
- VA Medical Facility—West Palm Beach, FL
- VA Medical Facility—White River Junction, VT

Vulnerability assessment 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 Audit Standards

The FISMA audit was conducted in compliance with Government Auditing Standards, July 2007 Revision, issued by the Comptroller General of the United States. The teams conducted their evaluations from April through September 2012. Standards for Performance Audits are applicable for this engagement. These standards require the teams plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for findings and conclusions based on the audit objectives. The evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objective.

Appendix D Acting Assistant Secretary for Information and Technology Comments

Department of Veterans Affairs

Memorandum

Date: May 30, 2013

From: Acting Assistant Secretary for Information and Technology (005)

Subj: Draft Audit Report: Federal Information Security Management Act (FISMA) Assessment for FY 2012

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

1. 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 to the report's 32 recommendations.

2. VA treats the protection of Veteran data very seriously. Toward that end, VA has embarked on a cultural transformation with implementation of the Continuous Readiness in Information Security Program (CRISP). CRISP is the new operating model for protecting our Veterans private and sensitive information. The program embodies an integrated approach to protecting sensitive information from inappropriate exposure or loss. Its framework depends on broad support to achieve many near-term goals in this fiscal cycle.

3. 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 Gary Stevens, Director, Office of Cyber Security, at 202-632-7538.

(original signed by:)

Stephen W. Warren

Attachment

Office of Information and Technology
Comments to Draft OIG Report,
"Federal Information Security Management Act Audit for FY 2012"
OIG Recommendations and OIT Responses:

Recommendation 1: We recommend the Acting Assistant Secretary 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 Technology (OIT) has established an Enterprise Risk Management (ERM) organization that 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.

OIT has also procured a Governance, Risk, and Compliance (GRC) tool and is currently implementing the product to facilitate the automated collection of certain risk management information. The GRC tool will be VA's sole repository capable of tracking the real-time security posture of the VA's IT systems, by exploiting existing IT monitoring and tracking tools, such as Tivoli End-Point Manager (TEM), SolarWinds, NESSUS, to extract, in real-time, up to 54 NIST controls, while capturing the remaining controls via automated workflows. The result is a more comprehensive understanding of the security posture of the VA far exceeding any past capabilities.

Target Completion Date: August 31, 2013

Recommendation 2: We recommend the Acting Assistant Secretary 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 Assistant Secretary for Information and Technology has implemented an interim solution, consisting of quarterly Plans of Action and Milestone (POAM) reviews as well as an external quality assurance assessment to ensure accurate supporting documentation for POAM closure. However, upon completion of the GRC tool, automatic processes are integrated into the framework, ensuring accuracy POAM closure justification is included in a centralized database.

Target Completion Date: August 31, 2013

Recommendation 3: We recommend the Acting Assistant Secretary 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. In tandem with the implementation of the GRC tool, VA has defined and implemented clear roles and responsibilities for the development, maintenance completion and reporting of all POAMs.

Target Completion Date: August 31, 2013 (tied to the implementation of the GRC tool)

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

OIT Response: Concur. With the implementation of the GRC tool which consists of continuous monitoring capabilities and automated vulnerability and configuration feeds, POAMs will be more accurately reflective of current status information.

Target Completion Date: August 31, 2013 (tied to the implementation of the GRC tool)

Recommendation 5: We recommend the Acting Assistant Secretary 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. VA established the OIT Security Calendar in 2012 which includes the annual updates to the System Security Plans. With the implementation of the GRC tool, a new mechanism for creating and maintaining system security plans will be established which will include reflection of ownership and operational environments. Many of the pieces within the system security plans will be automated, allowing for more accurate information to be maintained. A Continuous Readiness in Information Security Program (CRISP) Management Framework has been established to ensure verification and compliance.

Target Completion Date: March 31, 2014

Recommendation 6: We recommend the Acting Assistant Secretary 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. As with response to finding #5, new and improved processes for maintaining documentation such as risk assessments, security impact analyses and security self-assessments will be phased in consistent with the 3-year implementation plan of the GRC Tool. Many of the pieces within the documentation plans will be automated, allowing for more accurate information to be maintained. OIT will validate key security documents annually.

Target Completion Date: August 31, 2013

Recommendation 7: We recommend the Acting Assistant Secretary for Information and Technology implement mechanisms to enforce VA password policies and standards on all

operating systems, databases, applications, and network devices. (This is a repeat recommendation from last year.)

OIT Response: Concur. VA has implemented a process for monitoring password policies via predictive scans and remediation processes on OIT systems. Minimum requirements are in place to enforce VA passwords and standards on newer systems. VA's monthly predictive scanning process has drastically improved finding vulnerabilities with Password policies and is continually improving in this area.

Target Completion Date: January 31, 2014

Recommendation 8: We recommend the Acting Assistant Secretary for Information and Technology implement periodic access reviews to minimize access by system users with incompatible roles, permissions in excess of required functional responsibilities, and unauthorized accounts.

OIT Response: Concur. OIT has implemented quarterly reviews of all users with elevated privileges on IT Systems. Additionally, VA conducts semi-annual reviews of user accounts to ensure system users have the appropriate level of access and segregation of duties.

Target Completion Date: Complete and closed.

Recommendation 9: We recommend the Acting Assistant Secretary for Information and Technology enable system audit logs and conduct centralized reviews of security violations on mission-critical systems. (This is a repeat recommendation from 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. The installation of the devices for our field locations is contingent on funding in FY 2014.

Target Completion Date: September 30, 2014 (contingent upon receipt of funds)

Recommendation 10: We recommend the Acting Assistant Secretary for Information and Technology implement mechanisms to ensure all remote access computers have updated security patches and antivirus definitions prior to connecting to VA information systems. (This is a repeat recommendation from last year.)

OIT Response: Concur. A workgroup has been established to develop mechanisms to ensure all remote access computers have updated security patches and antivirus definitions prior to connecting to VA information systems.

Target Completion Date: January 31, 2014

Recommendation 11: We recommend the Acting Assistant Secretary for Information and Technology implement two-factor authentication for remote access throughout the agency. (This is a new recommendation.)

OIT Response: Concur. All users who require access to VA network resources will be required to utilize Two-Factor Authentication (2FA) for secure remote access by September 30, 2013.

Target Completion Date: September 30, 2013

Recommendation 12: We recommend the Acting Assistant Secretary 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 modified repeat recommendation from last year.)

OIT Response: Concur. VA has implemented predictive scanning beginning February 2013. This scanning allows for the identification of vulnerabilities, remediation of those vulnerabilities and compliance monitoring. Security Incident and Event Management (SIEM) Procurement by the NSOC is scheduled for FY14.

Target Completion Date: September 30, 2014

Recommendation 13: We recommend the Acting Assistant Secretary 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. VA implemented predictive scanning beginning February of 2013. This scanning allows for the identification of vulnerabilities, remediation of those vulnerabilities and compliance monitoring. A Security Management and Analytics office has been established and will continue to staff through September 2013 to monitor security deficiencies identified during our assessments of VA's Web applications, database platforms, network infrastructure, and work stations. Within Enterprise Operations, a consistent program for identifying and remediating vulnerabilities has been in place for several years.

Target Completion Date: June 30, 2013

Recommendation 14: We recommend the Acting Assistant Secretary 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 developed for enterprise level operating systems and platforms. Additional baselines are needed as new technology enters the environment. An intake process for this has been created and workflows/processes developed for this function. Known needed baselines include printers, thin clients, and SQL databases. These are being developed and will be completed by the target date.

Target Completion Date: September 30, 2013

Recommendation 15: We recommend the Acting Assistant Secretary 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. VA has implemented the Project Management Accountability System (PMAS) process and additional processes to address and enforce a system development and change control framework that integrates information security throughout the life cycle of each system. The Office of Cyber Security is in the process of coordinating with the relevant program offices to identify potential opportunities to inject security within the system development and change control framework.

Target Completion Date: September 30, 2014

Recommendation 16: We recommend the Acting Assistant Secretary 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 modified repeat recommendation from last year.)

OIT Response: Concur. Lessons learned were incorporated into the annual security calendar. A complete redesign was completed of the IS Contingency and Disaster Recovery documentation and testing processes in 2012. This redesign included the updating of required after action reports and lessons learned from Contingency and Disaster recovery testing.

Target Completion Date: September 30, 2013

Recommendation 17: We recommend the Acting Assistant Secretary 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. VA has identified the issue of backup tape encryption as a vulnerability. The Assistant Secretary for Information Technology has deferred a decision to ensure the encryption of backup tape data through a Risk Based Decision (RBD). This national RBD identifies mitigating controls to compensate the lack of backup tape encryption and will be further documented in local security documentation for systems that do not support backup tape encryption.

Target Completion Date: Completed

Recommendation 18: We recommend the Acting Assistant Secretary 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 that define the roles and responsibilities for alternate locations are in development.

Target Completion Date: June 30, 2013

Recommendation 19: We recommend the Acting Assistant Secretary 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 modified repeat recommendation from last year.)

OIT Response: Concur. Security Information & Event Management (SIEM) Procurement by the NSOC is scheduled for FY14.

Target Completion Date: September 30, 2014

Recommendation 20: We recommend the Acting Assistant Secretary 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 are currently under review (as part of OIT's annual review) and will be established or updated to reflect operational environments. As part of this effort, OIT issued a data call to report and document instances of air-gapped networks. OIT has documented these known connections (a new requirement) and has also published guidance on this subject.

Target Completion Date: September 30, 2013

Recommendation 21: We recommend the Acting Assistant Secretary for Information and Technology implement more effective agency-wide incident response procedures to ensure timely resolution of computer security incidents in accordance with VA set standards. (This is a modified repeat recommendation.)

OIT Response: Concur. VA has segregated the Network Security Operations Center into communications and cyber response components to allow more efficient and effective agency wide cyber incident response in order to ensure timely resolution of computer security incidents in accordance with VA set standards. Additional implementation involves a ticket escalation process to ensure that computer security events are being addressed timely.

Target Completion Date: September 30, 2013

Recommendation 22: We recommend the Acting Assistant Secretary for Information and Technology implement effective continuous monitoring processes to identify and prevent the use of unauthorized application software, hardware (including personal storage devices), and system configurations on its networks. (This is a repeat recommendation from last year.)

OIT Response: Concur. VA utilizes many tools such as Intrusion Protection System, Firewalls, Wireless Access Firewall, Tivoli Endpoint Management (Big Fix), anti-virus and Sanctuary to detect the presence and use of unauthorized software and hardware. The only item left to proactively monitor, prevent installation and remove unauthorized software is in development. The effort to design the solution is underway.

Target Completion Date: September 30, 2014

Recommendation 23: We recommend the Acting Assistant Secretary for Information and Technology develop a comprehensive software inventory process to identify major and minor software applications used to support VA programs and operations. (This is a repeat recommendation from last year.)

OIT Response: Concur. 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.

Target Completion Date: December 30, 2013

Recommendation 24: 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. Target Completion Date: August 30, 2013

Recommendation 25: We recommend the Acting Assistant Secretary for Information and Technology implement procedures for overseeing contractor managed systems and ensuring information security controls adequately protect VA sensitive systems and data. (This is a 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. OIT will work the TAC to ensure appropriate language is included in all OIT contracts.

Target Completion Date: Completed

Recommendation 26: We recommend the Acting Assistant Secretary for Information and Technology implement mechanisms for updating the Federal Information Security Management Act systems inventory, including interfaces with contractor-managed systems, 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 a 100% accuracy of its FISMA systems. At present, Tivoli 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. OIT will put in place a process to annually review the inventory for accuracy.

Target Completion Date: September 30, 2013

Recommendation 27: We recommend the Acting Assistant Secretary 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 modified repeat recommendation from last year.)

OIT Response: Concur. VA Deputy Secretary signed the CRISP Sustainment memo (VAIQ 7227211) that required all users of VA Computer systems and sensitive information be enrolled in the Talent Management System (TMS) by March 31, 2013. VA has maintained better than 97.6% compliance for Information Security Training.

Target Completion Date: Complete and Closed

Recommendation 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.

OIT Response - Status of Corrective Actions: With the implementation of the GRC Tool, new and improved processes for maintaining documentation such as risk assessments are being established. A percentage of the controls for each VA Information System (primarily those in the technical control family) will be monitored automatically and continuously, allowing for more accurate, complete, and timely information to be maintained. The GRC Tool will greatly improve the efficiency with which some controls are assessed, facilitating more timely risk management decision-making and enabling ongoing authorizations to operate. OIT is continuing to develop and refine an Information Security Continuous Monitoring (ISCM) program. OIT's ISCM program will not only address which controls will be monitored continuously via the GRC Tool, but will also include plans to periodically assess the remaining controls that cannot be automated and must continue to be assessed manually. Additionally, ERM will develop a program to periodically assess the automated tools providing input to the GRC Tool to ensure they are providing accurate and complete information.

Target Completion Date: September 30, 2013

Recommendation FY 2006–03: We recommend the Assistant Secretary for Information and Technology review and update all applicable position descriptions to better describe sensitivity ratings and better document employee personnel records and contractor files, including "Rules of Behavior" instructions, annual privacy and Health Insurance Portability and Accountability Act of 1996 training certifications, and position sensitivity level designations.

OIT Response - Status of Corrective Actions: The office responsible for this activity is the Office of Human Resources and Administration. The Assistant Secretary for Information Technology is actively partnering with the Office of Operations, Security and Preparedness and the Office of Human Resources and Administration to remediate this finding.

Target Completion Date: January 31, 2014

Recommendation 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.

OIT Response - Status of Corrective Actions: The office responsible for this activity is the Office of Operations, Security and Preparedness. The Assistant Secretary for Information Technology is partnering with the Office of Operations, Security and Preparedness and the Office of Human Resources and Administration to remediate this finding.

Target Completion Date: September 30, 2014

Recommendation FY 2006–08: We recommend the Assistant Secretary for Information and Technology reduce wireless security vulnerabilities by ensuring sites have an effective and up-to-date methodology to protect against the interception of wireless signals and unauthorized access to the network and ensure the wireless network is segmented and protected from the wired network.

OIT Response - Status of Corrective Actions: 50% of VA's wireless infrastructure has been upgraded to meet this requirement. The remaining 50% of the wireless enterprise is an unfunded but scheduled for funding in FY14.

Target Completion Date: September 30, 2014

Recommendation 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.

OIT Response - Status of Corrective Actions: VA is in the process of encrypting Desktops and Mobile Devices. Additional actions are under way to restrict the use of clear text protocols such as telnet and FTP.

Target Completion Date: September 30, 2013

Appendix E Office of Inspector General Contact and Staff Acknowledgements

OIG Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Acknowledgments	Michael Bowman, Director Carol Buzolich Elijah Chapman Neil Packard Richard Purifoy 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**.