VA Office of Inspector General

OFFICE OF AUDITS & EVALUATIONS

Department of Veterans Affairs

Federal Information Security Management Act Assessment for FY 2010

May 12, 2011
10-01916-165

ACRONYMS AND ABBREVIATIONS

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
[redacted]	[redacted]
[redacted]	[redacted]

b3, b7 (E)

To Report Suspected Wrongdoing in VA Programs and Operations:

Telephone: 1-800-488-8244

E-Mail: vaoighotline@va.gov

(Hotline Information: http://www.va.gov/oig/contacts/hotline.asp)

Department of Veteran Affairs

Memorandum

Date: May 3, 2011

From: Assistant Inspector General for Audits and Evaluations

Subj: Final Report: *Federal Information Security Management Act Assessment for FY 2010*

To: Assistant Secretary for Information and Technology

1. Enclosed is the final audit report, *Federal Information Security Management Act Assessment for FY 2010* (FISMA). The Office of Inspector General (OIG) contracted with the independent public accounting firms, Ernst & Young and Clifton Gunderson LLP to audit the Department's information security program in accordance with FISMA.

2. To ensure the adequacy and effectiveness of information security controls, FISMA requires agency program officials, Chief Information Officers, and Inspectors General to conduct annual reviews of the agencies' information security programs and report the results to the Office of Management and Budget (OMB). OMB 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 the FISMA objectives, 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 2010 consolidated financial statement audit; taking an agency-wide approach to successfully remediate high-risk issues through its Plans of Action and Milestones; establishing effective processes for evaluating information security controls via continuous monitoring and vulnerability assessments; and testing the effectiveness of corrective actions for closing recommendations and addressing problems though its Plans of Action and Milestones.

4. Ernst & Young was contracted to perform the FISMA assessment and is responsible for the findings and recommendations highlighted in the attached report dated April 29, 2011. The OIG does not express an opinion on the effectiveness of the Department's internal controls during FY 2010. Appendix A presents outstanding recommendations from previous assessments of the Department's information security program from FYs 2006 through 2009. Ernst & Young and the OIG assessed whether the Department's corrective actions successfully addressed the outstanding recommendations in FY 2010.

5. This report provides 34 recommendations, including two new ones, for improving the Department's information security program. Appendix A addresses the status of the recommendations from prior year assessments and the Department's plans for corrective action. Although you requested that three of the 40 outstanding recommendations be closed this year based on progress made, the OIG and Ernst & Young determined that eight recommendations have been successfully addressed; these recommendations are annotated as "closed" in Appendix A. The remaining recommendations have not been closed because relevant information security policies and procedures have not been finalized, or information security control deficiencies were repeated or newly identified during our FY 2010 FISMA assessment.
6. Our independent auditors will follow up on all outstanding recommendations and evaluate the adequacy of corrective actions during their FY 2011 FISMA assessment.
7. This report contains information protected from disclosure under the exemptions of the Freedom of Information Act. This unredacted report is for official use only and is not to be publicly disclosed without the approval of the Department of Veterans Affairs, Office of Inspector General.

(original signed by:)

BELINDA J. FINN
Assistant Inspector General
for Audits and Evaluations

Attachment

Ernst & Young LLP
8484 Westpark Drive
McLean, Virginia 22102
Tel: +1 703 747 1000
Fax: +1 703 747 0100
www.ey.com

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

April 29, 2011

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, 2010 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.

Ernst & Young was contracted to perform the FISMA assessment and is responsible for the findings and recommendations highlighted in the attached report. We conducted this performance audit in accordance with Government Auditing Standards ("GAS") developed by the Government Accountability Office ("GAO"). 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 Ernst & Young and approved by the Office of the Inspector General (OIG), during the period March 2010 through October 2010. 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 Clifton Gunderson 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 additions to the findings and recommendations, our conclusions related to VA are contained within the OMB FISMA reporting template provided to the OIG in November 2010.

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 Ernst & Young.

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,

Ernst & Young LLP

Report Highlights: Federal Information Security Management Act Assessment for FY 2010

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 2010 annual FISMA assessment determined the extent to which VA's information security program complied with FISMA requirements and applicable National Institute for Standards and Technology information security guidelines. We contracted with the independent accounting firms Ernst & Young and Clifton Gunderson LLP to perform the FY 2010 FISMA assessment.

What We Found

VA has made progress developing policies and procedures, but still faces challenges implementing components of its agency-wide information security program to meet FISMA requirements. FISMA assessments 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.

Specifically, VA has not enforced password complexity standards on all servers and network devices, resulting in weak or default user passwords on critical systems. Also, VA has not effectively implemented procedures to identify and remediate system security vulnerabilities on network devices, database and server platforms, and Web applications across the enterprise.

Further, VA has not remediated more than 13,000 outstanding system security risks and corresponding Plans of Action and Milestones to improve its overall information security posture. As a result of the FY 2010 consolidated financial statement audit, Clifton Gunderson LLP concluded a material weakness exists in VA's information security program.

What We Recommend

This report provides 34 recommendations for improving VA's information security program. We recommend the Assistant Secretary for Information and Technology implement comprehensive procedures to mitigate security vulnerabilities affecting VA's mission-critical systems.

Agency Comments

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

(original signed by:)

BELINDA J. FINN
Assistant Inspector General
for Audits and Evaluations

Table of Contents

INTRODUCTION

Objective

We determined the extent to which VA's information security program and practices comply with Federal Information Security Management Act (FISMA) requirements, Office of Management and Budget (OMB) reporting requirements, and applicable National Institute for Standards and Technology (NIST) guidance. We contracted with the independent accounting firms Ernst & Young and Clifton Gunderson LLP to perform the FY 2010 FISMA assessment.

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. The audit teams assessed the Department's information security program through inquiries, observations, and tests of selected controls supporting 80 major applications and general support systems at 23 VA facilities. The teams identified specific deficiencies in the following areas:

A. Agency-Wide Security Program
B. Identity Management and Access Controls
C. Configuration Management Controls
D. System Development/Change Management Controls
E. Contingency Planning
F. Incident Response
G. Continuous Monitoring
H. Certification and Accreditation
I. Security Awareness Training
J. System Inventory
K. Contractor System Oversight

This report provides 34 recommendations to the Assistant Secretary for Information and Technology for improving VA's information security program. Appendix A addresses the status of recommendations from prior year assessments and VA's plans for corrective action. During FY 2010, VA successfully addressed eight prior year recommendations; these recommendations are annotated as "closed" in Appendix A.

RESULTS AND RECOMMENDATIONS

Finding 1 Agency-Wide Security Program

FISMA requires each Federal agency develop, document, and implement an agency-wide information security 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 program to meet FISMA requirements. FISMA assessments 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

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 program. During 2010, VA continued meeting major milestones and further defined agency-wide information security objectives by issuing additional directives and handbooks:

- Handbook 6500.8, *Information Technology Contingency Planning* (November 2009)
- Directive 6512, *Secure Wireless Technology* (November 2009)
- Handbook 6502.4, *Privacy Act Review* (November 2009)
- Handbook 6500.6, *Contract Security* (March 2010)
- Handbook 6500.5, *Incorporating Security and Privacy into the System Development Life Cycle* (March 2010)
- Handbook 6300.1, *Records Management Procedures* (March 2010)
- Handbook 6300.5, *Procedures for Establishing and Managing Privacy Act Systems of Records* (June 2010)
- Directive 6513, *Secure External Connections* (July 2010)
- Directive 6371, *Destruction of Temporary Paper Records* (October 2010)

Further, VA devoted considerable resources to identify information system security risks through its Certification and Accreditation program. In 2010, VA certified and accredited about one-third of its approximately 620 major applications and general support systems, as annually required. As part of this certification and accreditation effort, it also partially implemented a new risk assessment template, addressing previous deficiencies identified by the OIG. VA continued improving systems and data security control protections by implementing technological solutions, such as secure remote access, application filtering, and portable storage device encryption. VA began its "Visibility to the Desktop" initiative, which allows central monitoring of all

end-user computers connected to the network. Additionally, VA developed security configuration policy for several Microsoft platforms to reduce risks associated with default computer settings that can be exploited by attackers.

Ongoing Challenges

VA has not yet implemented all of the information security controls needed to comply with FISMA requirements. FISMA Section 3544 requires agencies implement a process for planning, implementing, evaluating, prioritizing, and documenting remedial actions to address deficiencies in the agency's information security policies, procedures, and practices. OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Actions and Milestones* (POA&Ms), defines management and reporting requirements for agency POA&Ms, including deficiency descriptions, remediation actions, required resources, and responsible parties.

Despite these requirements, assessment teams continue to identify significant deficiencies related to POA&Ms for addressing access controls, configuration management controls, change management controls, and service continuity controls to protect mission-critical systems from unauthorized access, alteration, or destruction.

Further, Office of Information and Technology assessments have identified more than 13,000 outstanding POA&M actions that must be taken to remediate risks and improve VA's information security posture. Assessment teams identified numerous POA&Ms that lacked sufficient documentation to justify closure of action items. A number of system security weaknesses had not been remediated from the prior year. Assessment teams also identified more than 300 POA&M actions that had missed major milestones and had not been updated to reflect their current status.

A number of these POA&M deficiencies were due to insufficient controls to verify appropriate supporting documentation had been input to the [redacted] to track and report POA&M issues. For example, VA has not defined clear roles and responsibilities for creating, uploading, updating, and closing POA&M items in [redacted] Unclear responsibility for managing POA&M records has adversely impacted remediation efforts across the enterprise. By failing to remediate a large number of its 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 [redacted] to justify POA&M action item closures, VA cannot assure that corresponding security risks have been fully mitigated. b3, b7(E)

Recommendations

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

2. *We recommend the Assistant Secretary for Information and Technology implement control mechanisms to ensure sufficient supporting documentation is captured in the [redacted] to justify Plans of Action and Milestones closures. (This is a repeat recommendation from last year.)* b3, b7(E)

3. *We recommend the Assistant Secretary for Information and Technology define and implement clear roles and responsibilities for developing, maintaining, completing, and reporting Plans of Action and Milestones in accordance with Office of Management and Budget Memorandum M-02-01.*

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

Finding 2 Identity Management and Access Controls

Comprehensive identity management and access controls are designed to protect VA's major applications and general support systems from unauthorized access, alteration, and destruction. We identified significant information security control weaknesses with major applications and general support systems in five areas:

- Password Management
- Access Management
- Audit and Accountability
- Remote Access
- Virtual Local Area Network

Password Management

VA Handbook 6500, Appendixes D and F establish minimum systems security controls and password management standards for authenticating VA system users. Assessment teams identified 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 several major [redacted] and [redacted] were not configured to enforce VA's password complexity and policy standards. Specific deficiencies include the following.

- Numerous mission-critical servers and [redacted] contained the same user names and passwords, default passwords, and easily-guessed passwords.
- Numerous servers and network devices contained default simple network management protocol community strings and default administrator level passwords.
- Database password policy settings for many [redacted] and [redacted] were not set in accordance with VA policy standards. b3, b7(E)
- Domain Controller settings, such as concurrent log-in sessions and audit policies, did not comply with VA policy standards.
- Domain Controller settings stored user password hashes via the local area network authentication mechanism, increasing the risk that user credentials could be intercepted for malicious use.
- [redacted] password parameter settings, such as concurrent log-in sessions and account lockout policy, did not comply with VA policy standards.
- Numerous [redacted] operating system user accounts contained passwords that did not comply with VA complexity requirements, including password length and expiration settings.

VA has not developed effective controls to ensure compliance with password complexity standards on major applications and general support systems. The use of weak passwords is a well-known security vulnerability that allows malicious users to easily gain unauthorized access to mission-critical systems. VA is conducting an executive review of the implications of implementing a 16-character password complexity standard across the enterprise.

Access Management

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. Specifically, we identified the following.

- At two VA facilities, more than 30 terminated employee user accounts had not been disabled or removed from network resources. Five of these accounts were subsequently used to access VA network resources after the end-user separation date.
- VA facility application developers typically have access to both application production and test environments, increasing the risk of unauthorized changes to mission-critical systems.
- Most VA medical facilities had a significant number of users with incompatible privileges, such as both creating and approving Purchase Orders and obligating funds within [redacted]. Excessive permissions increase the risk of fraudulent transactions. b3, b7(E)
- Numerous generic user accounts existed on applications and network resources. Use of generic accounts does not ensure full accountability for user activity on critical systems.
- More than 120 users had the ability to perform system administrator functions within [redacted] via [redacted] and [redacted] menu access. Use of powerful systems functions should be restricted to a minimum number of users.
- Numerous [redacted] user accounts were members of the "All" privileges group, allowing those users to add, delete, copy, or modify any system data hosted on [redacted] Use of powerful systems functions should be restricted to a minimum number of users.
- More than 20 end-users were granted access to mission-critical systems without first obtaining proper authorization. Formal access approvals are needed to ensure users gain access to critical resources only as appropriate.
- More than 250 inactive user accounts had never been used to log onto network resources and had not been disabled. Inactive user accounts provide attackers with opportunities to gain unauthorized access to critical systems.
- Several unauthorized wireless access points could be used to gain inappropriate access to VA networks and critical systems.

VA has not implemented effective reviews to eliminate such instances of unauthorized system access and 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. 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. VA Handbook 6500, Appendix D provides high-level policy and procedures for collection and review of system 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 systems performance issues.

Remote Access

VA lacks a consistent process for managing remote access to VA networks. VA Handbook 6500, Appendix D establishes high-level policy and procedures for managing remote connections. However, users can log onto VA networks using either [redacted] or [redacted] both [redacted] for encrypted remote access. [redacted] solution 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. b3, b7(E)

Network Segmentation

The majority of VA's sensitive medical devices or other network segments remain unprotected. Virtual Local Area Networks are intended to restrict access to sensitive medical device networks and are critical for the security and operational stability of medical centers. However, assessment teams gained unauthorized access to a number of sensitive logical networks at VA facilities. VA is implementing logical network separation of workstations, printers, and servers through Virtual Local Area Network access control mechanisms to prevent such unauthorized connections in the future.

Recommendations

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

6. *We recommend the Assistant Secretary for Information and Technology implement periodic access reviews to minimize access by system users*

with incompatible roles, permissions in excess of required functional responsibilities, and unauthorized accounts. (This is a modified repeat recommendation from last year.)

7. *We recommend the Assistant Secretary for Information and Technology enable system audit logs and conduct centralized reviews of security violations on mission-critical systems. (This is a modified repeat recommendation from last year.)*

8. *We recommend the Assistant Secretary for Information and Technology implement mechanisms to ensure all remote access computers have updated security patches and antivirus definitions prior to connecting to VA information systems.*

9. *We recommend the Assistant Secretary for Information and Technology implement effective Virtual Local Area Network controls to eliminate unauthorized access to sensitive network segments. (This is a modified repeat recommendation from last year.)*

Finding 3 Configuration Management Control

Assessment teams identified significant weaknesses in configuration management controls designed to protect VA's critical systems from unauthorized access, alteration, or destruction. VA Handbook 6500, Appendix D provides high-level policy regarding mandatory configuration settings and related documentation 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. VA is developing a new appendix to the handbook to define agency-wide configuration management policy and change control procedures for integration of security controls throughout the life cycle of each system.

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 exploit vulnerabilities and gain unauthorized access to VA information systems. For example, an attacker could potentially alter sensitive data or covertly run unauthorized programs on Web applications. Testing identified the following Web application vulnerabilities.

- Sixteen Web applications were vulnerable to [redacted] or [redacted] attacks, enabling attackers to bypass access controls and obtain sensitive system information. b3, b7(E)
- Seven Web applications were vulnerable to [redacted] attacks through which unauthorized individuals could retrieve sensitive information.
- Twelve Web applications did not encrypt user account credentials, which could compromise user passwords and provide attackers with easy access to critical systems.
- Ten Web applications stored passwords [redacted] increasing the risk of attackers obtaining system passwords and sensitive information.
- Four Web applications were using outdated encryption modules that did not comply with Federal Information Processing Standards.

VA has not implemented effective controls to identify and remediate such security weaknesses on its 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." While VA has mitigated some information system security risk from the Internet

through the use of network filtering appliances, VA's internal network remains susceptible to attack from malicious users.

Unsecure Database Applications

Database vulnerability assessments identified a significant number of unsecure configuration settings that could allow any database user to gain unauthorized access to critical system information. Specific database vulnerabilities include the following.

- Twenty-four [redacted] and [redacted] were missing critical patches and system software updates. These weaknesses could allow malicious users to gain administrator rights to the database and modify or delete critical files and information. b3, b7(E)
- Thirteen [redacted] that support critical systems provided excessive permissions to [redacted] users, including the following—library creation, system registry execution, link table access, and [redacted] database management service access. Any [redacted] user could use these permissions to gain administrator rights on the [redacted] or access to the underlying operating system.
- One [redacted] hosting [redacted] sensitive data contained clear text default passwords and provided numerous default services that could allow unauthorized users to access [redacted] For instance, the database was configured to allow any user to access the system registry and obtain all users' credentials on the system.

VA has not implemented effective controls to identify and remediate security weaknesses on databases hosting mission-critical applications. 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. This principle can be applied to databases as well.

Application and System Software Vulnerabilities

Network vulnerability assessments identified a significant number of outdated operating systems and vulnerable third-party applications that could allow unauthorized access to mission-critical systems and data. Some significant security vulnerabilities include:

- Numerous servers hosting [redacted] management applications with outdated application security patches and default passwords. These security weaknesses provide well-known opportunities for unauthorized access or destruction of VA sensitive data through means such as buffer overflow attacks.
- Numerous servers hosting outdated [redacted] services. These services are vulnerable to arbitrary code execution, providing potential unauthorized access to the server operating system.

- Numerous servers hosting outdated versions of backup recovery software, such as [redacted] and [redacted] A malicious user could exploit flaws in the software to gain administrator rights on the server and obtain user passwords to attack other systems.

VA has not implemented effective controls to identify and remediate security weaknesses associated with outdated third-party applications and operating system software. NIST Special Publication 800-40, Version 2, *Creating a Patch and Vulnerability Management Program,* states a patch and vulnerability management program should be integrated with configuration management to ensure efficiency. A robust patch and vulnerability management program would enable the Department to effectively remediate vulnerabilities identified in operating systems, databases, applications, and other network devices.

Baseline Security Configurations

VA is developing guidelines to define agency-wide configuration management policy and change control procedures. However, common platform security standards and [redacted] are not fully implemented on all VA systems. Testing at VA facilities revealed 70 to 90 percent of Federal Desktop Core Configuration standards have been applied to 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 [redacted]'s operating system. b3, b7(E)

FISMA Section 3544 requires each agency to develop minimally acceptable system configuration requirements and ensure compliance. Without implementing agency-wide configuration management standards for major applications, general support systems, and end-users, VA is placing critical systems at unnecessary risk of unauthorized access, alteration, or destruction.

Recommendations

11. *We recommend the Assistant Secretary for Information and Technology implement automated mechanisms to continuously identify and remediate security weaknesses on VA's network infrastructure, database platforms, and Web application servers. (This is a repeat recommendation from last year.)*

12. *We recommend the Assistant Secretary for Information and Technology implement a patch and vulnerability management program to address security weaknesses identified during our assessments of VA's Web applications, database platforms, and network infrastructure. (This is a modified repeat recommendation from last year.)*

13. *We recommend the Assistant Secretary for Information and Technology develop and implement standard security configuration baselines for all VA operating systems, databases, applications, and network devices. (This is a modified repeat recommendation from last year.)*

Finding 4 System Development/Change Management Control

VA has not 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 (March 2010)* also discusses integrating information security controls and privacy throughout the life cycle of each system.

Our assessment teams determined that software changes to [redacted] b3, b7(E) did not follow standardized software change control procedures. Further, many 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

14. We recommend the 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

VA Handbook 6500, Appendix D establishes high-level policy and procedures for contingency planning and plan testing. Our assessments identified many contingency plans that were not completely tested; test results also were not clearly documented or effectively communicated to senior management. Specific deficiencies include:

- Many contingency plans lacked required information, such as Business Impact Analysis data, accurate hardware and software inventories, alternate site agreements, vendor service-level agreements, and detailed system backup and reconstitution procedures. In some cases, the alternate processing sites were located in the same geographic regions as the primary data hosting facilities.
- In most cases, contingency plan testing did not validate whether system owners could restore those systems at alternate processing sites. Some locations performed table-top testing—a discussion-based exercise that does not involve deploying equipment or resources—as a substitute for full contingency plan testing.

VA has not implemented contingency plan testing in accordance with its security requirements. Incomplete documentation of plans and test results may 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. Further, inadequate communication of test results to senior management may prevent lessons learned from being recognized and adopted.

Recommendation

15. *We recommend that the Assistant Secretary for Information and Technology implement processes to ensure information system contingency plans are updated with the required information, plans are fully tested at alternate processing facilities, and lessons learned are communicated to senior management. (This is a modified repeat recommendation from last year.)*

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 develop and implement an agency-wide information security program containing specific procedures for detecting, reporting, and responding to computer security incidents.

In line with this requirement, VA performs a significant amount of monitoring at its known Internet gateways. This monitoring includes some event correlation, which is the process of tying multiple monitoring entries together to identify larger trends, intrusions, or intrusion attempts. This process is designed to alert VA's [redacted] when a security event occurs and exceeds certain thresholds in terms of significance.

However, VA has not fully implemented security information and event management technology to perform effective correlation analysis. Most network security events are evaluated manually, which is inadequate to monitor and manage VA's numerous and complex network connections. Assessments teams also identified several system interconnections without required Interconnection Security Agreements and Memoranda of Understanding to govern them. b3, b7(E)

Ineffective monitoring of external network interconnections could prevent VA from detecting and responding to an intrusion attempt in a timely manner. In efforts to improve incident management, VA's [redacted] is implementing its Trusted Internet Connection initiative to identify all system interconnections and consolidate them into four VA gateways. Management estimates more than 460 external network connections and approximately 290 of those connections are routed through the [redacted] and are actively monitored. Although progress has been made in cataloging the many interconnections for monitoring purposes, unknown connections still exist.

Recommendations

16. *We recommend the Assistant Secretary for Information and Technology implement technological solutions to monitor security for all systems interconnections and network segments supporting VA programs and operations. (This is a repeat recommendation from last year.)*

17. *We recommend the Assistant Secretary for Information and Technology identify all external network connections and ensure appropriate Interconnection Security Agreements and Memoranda of Understanding are in place to govern them. (This is a repeat recommendation from last year.)*

Finding 7 Continuous Monitoring

VA lacks a continuous monitoring process to effectively identify its hardware and software inventory, perform automated monitoring of its networks, and test security controls. NIST Special Publication 800-53, Revision 3 outlines the importance of deploying automated mechanisms to detect unauthorized components and devices within agency networks. However, [redacted] have not implemented the technology needed to actively monitor their networks for unauthorized software and hardware devices. b3, b7(E)

For example, VA personnel can connect to mission-critical systems using unencrypted thumb drives and exchange sensitive information. Unauthorized hardware and software components introduce vulnerabilities that could jeopardize network integrity. VA has partially implemented software to prevent connections of unencrypted storage devices; however, this software is not deployed to all VA facilities. Our technical testing also continues to identify significant weaknesses with configuration management controls designed to protect mission-critical systems from unauthorized access, alteration, or destruction.

Recommendation

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

Finding 8 Certification and Accreditation

VA continued its initiative to certify and accredit approximately a third of its major applications and general support systems in advance of the 3-year time interval requirement. However, testing identified a number of certification and accreditation packages that were in draft format and contained outdated system security plans, risk assessments, and security control assessments. VA Handbook 6500, Appendix D establishes the high-level policy and procedures for developing system security plans, conducting risk assessments, and maintaining system security plans in connection with the certification and accreditation process.

System Security Plans

System security plans should be periodically updated based on the results of assessments or modifications to system security controls. Assessment teams identified many system security plans lacking required information or containing the following deficiencies:

- Outdated information regarding operational environments, system test results, system interconnections, and system ownership.
- Incomplete information regarding existing and compensating information security controls.
- Inaccurate inventories of hardware, software, and application platforms supporting the information systems.

Because of these deficiencies, system owners cannot identify relative boundaries, interdependencies, and potential security risks impacting mission-critical systems. Further, without updating system security plans with security control test results, analysis of related compensating controls, and relevant risk-based decisions, officials are not fully aware of residual security risks at the time they formally authorize systems to operate.

Risk Assessments

VA's revised Risk Assessment Template aligns with guidelines in NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*. Through the new template, VA enhanced security control descriptions for major applications and general support systems and identified control deficiencies for remediation. However, VA has not evaluated a significant number of systems using the newly adopted risk assessment process; therefore, many security documentation deficiencies from previous years remain.

Specifically, risk assessments using the legacy process did not include analysis of mitigating controls that could reduce or eliminate the identified security risks. Without accurately assessing the effectiveness of security controls during the risk assessment process, system owners could not effectively determine relative threats and vulnerabilities to VA systems. Additionally, system owners did not identify the appropriate compensating

controls to minimize or eliminate the identified risks. As a result, critical vulnerabilities may not be resolved in a timely manner, placing VA systems at unnecessary risk of unauthorized access, alteration, or destruction.

Recommendations

19. *We recommend that the Assistant Secretary for Information and Technology develop mechanisms to ensure system security plans reflect current operational environments, including accurate inventories of systems, software, database platforms, and system interconnections. (This is a modified repeat recommendation from last year.)*

20. *We recommend that the Assistant Secretary for Information and Technology develop mechanisms to ensure system security plans are updated to reflect results of security control and analysis testing, compensating control evaluations, and residual risk-based decisions. (This is a modified repeat recommendation from last year.)*

21. *We recommend that the Assistant Secretary for Information and Technology implement revised risk assessment processes across the enterprise to effectively identify threats to and vulnerabilities of major applications and general support systems. (This is a modified repeat recommendation from last year.)*

22. *We recommend that the Assistant Secretary for Information and Technology develop mechanisms to ensure risk assessments accurately reflect the current control environment, compensating control recommendations, and the characteristics of the relevant VA facilities. (This is a repeat recommendation from last year.)*

Finding 9 Security Awareness Training

VA does not have automated processes in place to track security awareness training for residents, volunteers, and contractors at VA facilities. VA Handbook 6500, Appendix D establishes high-level policy and procedures for a security awareness training program. This program requires all users of sensitive information annually complete VA's security awareness training. VA utilizes the [redacted] an online training application, to track required security awareness and other training and provide user access to a number of online training resources. b3, b7(E)

While the [redacted] is effective in tracking VA employee training, VA relies on a manual processes for tracking training requirements for residents, volunteers, and contractors. Without automated tracking that would enable centralized monitoring and more complete and accurate reporting, management cannot assure that these personnel have completed the annual security awareness training requirements.

Further, our testing identified numerous personnel with significant information technology responsibilities who had not completed specialized training at VA facilities. VA Handbook 6500, Appendix D includes high-level policy and procedures for managing and implementing such a specialized training program. In 2010, Information Security Officers participated in specialized technical training. However, employees such as information technology specialists, system administrators, and database administrators did not complete specialized training that year. VA did not effectively communicate requirements or manage its role-based training program. As such, training administrators were not aware of the specialized role-based training curriculum provided within the [redacted] Computer security awareness training and specialized security training are essential to help employees and contractors understand information security and privacy issues and obtain the skills needed to protect VA systems and data.

Recommendations

23. *We recommend that the Assistant Secretary for Information and Technology implement mechanisms to ensure all contractors and other users with VA network access participate in and complete required VA-sponsored security awareness training. (This is a modified repeat recommendation from last year.)*

24. *We recommend that the Assistant Secretary for Information and Technology identify and ensure personnel with specialized security responsibilities fulfill annual specialized computer security training requirements. (This is a modified repeat recommendation from last year.)*

Finding 10 System Inventory

This year's assessment identified some inaccuracies in the Department's system inventory. VA Handbook 6500, Appendix D defines information systems inventory requirements. The Office of Cyber Security maintained its inventory of information systems within [redacted] the centralized system of record for FISMA reporting purposes. However, the [redacted] systems inventory did not identify interfaces between contractor-managed systems and VA internal networks as FISMA required. Unidentified contractor systems and interconnections could pose significant risks to VA networks and operations if not evaluated and mitigated by compensating controls. b3, b7(E)

Further, VA uses the [redacted] to inventory hardware at its medical facilities. However, VA has not developed a similar process at the medical facilities to identify the software components supporting critical programs and operations. Incomplete listing of critical software components may prevent restoration of services in the event of a system disruption or disaster.

Recommendations

25. *We recommend the Assistant Secretary for Information and Technology implement mechanisms for updating the [redacted] systems inventory, including interfaces with contractor-managed systems, and annually review the systems inventory for accuracy. (This is a modified repeat recommendation from last year.)*

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

Finding 11 Contractor Systems Oversight

In 2010, VA did not fully implement contractor oversight procedures as required. According to FISMA Section 3544, an agency should ensure information security for the systems that support their operations, including those provided by another agency, contractor, or other source. VA developed and published VA Handbook 6500.6, *Contract Security,* in March 2010, providing detailed guidance on contractor systems oversight and establishing security requirements for all its contracts involving sensitive VA information.

VA launched a series of education campaigns to communicate its new contractor oversight procedures. VA also initiated site assessments to determine whether contractors were complying with its contract security requirements. VA anticipates completing 5 percent of these site assessments by the end of FY 2011. Despite these improvements, our assessment disclosed several deficiencies in VA's contractor oversight activities in 2010.

- Two contractor-[redacted] had not undergone an annual security controls assessment as required by FISMA. b3, b7(E)
- Ten contractor-[redacted] had not performed contingency planning tests.

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.

Recommendation

27. *We recommend that the 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 modified repeat recommendation from last year.)*

Summary of Response - Assistant Secretary for Information and Technology

The Department concurred with all findings and recommendations and prepared a response which is presented in Appendix D. The Assistant Secretary for Information and Technology stated that VA continues to make progress in improving the effectiveness of its information security program and system security controls through issuance of policy directives and implementing technological solutions such as remote access, portable storage device encryption, and the visibility to the desktop initiative. The Assistant Secretary also noted the establishment of the FISMA Challenge Team that will address solutions for outstanding Plans of Actions and Milestones. The OIG will continue to evaluate VA's progress during our assessment of the Department's information security program in FY 2011.

Appendix A Status of Prior Year Recommendations

Appendix A documents the status of recommendations from our FISMA assessments for FYs 2006 through 2009. As noted in the table below, certain recommendations are closed because of updated recommendations presented in this report. The corrective actions outlined below are based on management assertions and results of our assessment testing. In FY 2010, VA successfully addressed eight recommendations, as indicated in the table.

Number	Recommendation	Assessment Status	Estimated Completion	Corrective Actions
FY09-13	We recommend that the Assistant Secretary for Information and Technology, in conjunction with the Office of the Secretary and the Office of Public and Intergovernmental Affairs, develop and test continuity of **operations** plans in accordance with VA Directive and Handbook 0320, *Comprehensive Emergency Management Program.*	In progress	To Be Determined	The Department has recently updated the Master Continuity of Operations Plans to include all the necessary components. However, some plans were not updated during the past year.
FY09-21	Develop and implement mechanisms for ensuring POA&Ms are remediated and documented in accordance with VA Handbook 6500.	Closed See updated recommend-ation10-02 for this year.	Not Applicable	
FY09-27	We recommend that the Assistant Secretary for Information and Technology, in conjunction with the Deputy Assistant Secretary for Acquisition and Materiel Management, implement procedures to ensure that Department contracts contain information security compliance clauses consistent with FISMA requirements.	Closed	Not Applicable	VA Handbook 6500.6, *Contract Security*, was issued in March 2010. It provides guidance on procedures for ensuring VA contracts contain information security compliance clauses consistent with FISMA requirements. No exceptions were noted.

Number	Recommendation	Assessment Status	Estimated Completion	Corrective Actions
FY08-10	Communicate the importance of reporting computer security incidents so local management can effectively mitigate system security risks.	Closed	Not Applicable	VA Handbook 6500.2, *Management of Security and Privacy Incidents*, was issued in June 2008. No exceptions were noted.
FY08-18	Ensure that user access to the [redacted] database is assigned based on individual need and periodically reviewed for unauthorized access.	Closed	Not Applicable	User reviews were conducted for continued access to the [redacted] database. No exceptions were noted.
FY07-04	Implement VA Directive 6330 and information security management policy and procedures in accordance with FISMA requirements.	Closed	Not Applicable	The Chief Information Officer signed and implemented an updated VA Directive 6330 on 2/26/2009. No exceptions were noted.
FY07-30	Enhance VA Handbook 6500 to include policy and procedures for the Network Security Operations Center's role in governing systems interconnections.	Closed See updated recommend-ation 10-15 for this year.	To Be Determined	VA Directive 6513, *Secure External Connections*, published in 2010, provides policy and procedures for the Network Security Operations Center's role in governing systems interconnections.
FY07-31	Implement policy and procedures to govern systems interconnections, with consideration to NIST Special Publication 800-47.	Closed See updated recommend-ation 10-16 for this year.	To Be Determined	VA is implementing Directive 6513.

b3, b7(E)

Number	Recommendation	Assessment Status	Estimated Completion	Corrective Actions
FY06-03	Review and update all applicable position descriptions to better describe sensitivity ratings, and better document employee personnel records and contractor files to include "Rules of Behavior" instructions, annual privacy, Health Insurance Portability and Accountability Act of 1996 training certifications, and position sensitivity level designations.	In progress	To Be Determined	VA has implemented the [redacted] Department-wide. The Personnel Security and Suitability Service has met with Veterans Health Administration and Veterans Benefits Administration human resource managers and provided them with the proper information to utilize the tool. VA Notice 09-02, issued on March 24, 2009, replaced VA Form 2280, *Position Risk and Sensitivity Level Designation*, and VA Form 2280a, *Contractor Position Risk and Sensitivity Level Designation*. Notice 09-02 establishes the *Position Designation Record*, which simplifies position designation and provides an automated method for making these determinations. The guidance issued in the notice remains in effect until formally issued through the Directive and Handbook 0710: Personnel Suitability and Security Program. The Directive and Handbook have not been finalized.

b3, b7(E)

Number	Recommendation	Assessment Status	Estimated Completion	Corrective Actions
FY06-04	Timely request the appropriate levels of background investigations on all applicable VA employees and contractors. Additionally, monitor and ensure timely requests for reinvestigations on all applicable employees and contractors. Monitor the status of the requested investigations.	In progress	To Be Determined	The Security Center located in Little Rock, AR uses a MicroSoft Access database to track when cases are sent to the Office of Personnel Management, when they are returned for corrections, and when they are adjudicated. Part of the process includes sending out a daily status of VA Background Investigations to the Deputy Director for National Security Programs Investigations. The [redacted] is the electronic questionnaire for processing applicant investigations. Every 2 weeks the system sends out reminders to applicants to complete their package. This reminder serves to keep the applicants on track in submitting their Background Investigation forms. Exceptions were noted during testing.
FY06-07	Strengthen physical access controls to correct previously reported physical access control deficiencies, develop consistent standardized physical access control requirements, policies, and guidelines throughout VA, and limit computer room access to individuals with a legitimate need.	In Progress	To Be Determined	VA Directive and Handbook 0730 implementation has been placed on hold pending the outcome of updated safety and security vulnerability assessments.

b3, b7(E)

Number	Recommendation	Assessment Status	Estimated Completion	Corrective Actions
FY06-08	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. Additionally, 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 a methodology for protecting VA wireless networks from signal interception, enhancing network security, and segmenting the wireless network from VA's wired network. VA's Wireless Local Area Network Security Standards Policy is applicable to all wireless networks attached to any segment of VA's network, administered by the Office of Information and Technology. The policy provides guidance on how wireless networks are segmented from the wired network, identifies possible exceptions, details the configuration of wireless segments, and establishes requirements for penetration testing and auditing of the network to ensure compliance with network segmentation and security requirements. Exceptions were noted during testing.

Number	Recommendation	Assessment Status	Estimated Completion	Corrective Actions
FY06-09	Identify and deploy solutions to encrypt sensitive data and resolve clear text protocol vulnerabilities.	In progress	To Be Determined	Multiple technologies are being developed, integrated, and deployed across VA's enterprise to encrypt sensitive data, both at rest and in transit: • [redacted] deployment to ensure only USB-devices are in use is 20 percent complete. . • Remote Enterprise Security Compliance Update Environment user migration is 30 percent complete. • Laptop and thumb drive encryption have been deployed. • Tape encryption testing is underway at four VA sites: [redacted] Clear text protocol vulnerabilities were identified during our 2010 FISMA testing.

b3, b7(E)

Number	Recommendation	Assessment Status	Estimated Completion	Corrective Actions
FY06-12	Develop and fully implement procedures for protecting sensitive information accessed remotely or removed from VA facilities in accordance with NIST Special Publication 800-53.	In-Progress	To Be Determined	The [redacted] is in the process of deploying intrusion detection systems throughout the VA network and implementing means to monitor all remote devices. [redacted] can be connected to the network and used to download sensitive information.
FY06-13	Complete the implementation of two-factor authentication in accordance with NIST Special Publication 800-53.	In progress	To Be Determined	VA will define program milestones for Identity Management, Access Control, and Separation of Duties. VA has not fully implemented two-factor authentication throughout the enterprise.
FY06-15	Complete implementation of security control measures involving access to sensitive information by non-VA employees.	Closed See updated recommend-ation 10-26 for this year.	Not Applicable	VA has completed or begun implementation of several technical initiatives to protect its sensitive information. While not all inclusive, these are described in VA's responses to recommendation FY06-09.

b3, b7(E)

Appendix B Background

On December 17, 2002, the President 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 the National Institute of Standards and Technology 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 provides instructions to Federal agencies and Inspectors Generals for preparing annual FISMA reports. OMB's reporting instructions 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, testing contingency plans, and certifying and accrediting systems. Per OMB instruction, the OIG must assess the effectiveness of VA's information security program and practices on an annual basis. The OIG contracted with the independent accounting firms Ernst & Young and Clifton Gunderson LLP to conduct the annual FISMA assessment for FY 2010. The OIG provided oversight of the contractors' performance.

Appendix C Scope and Methodology

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

This year's assessment included evaluation of 80 selected major applications and general support systems hosted at 23 VA facilities to support Veterans Health Administration, Veterans Benefit Administration, and National Cemetery Administration lines of business. The assessment 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 2010 consolidated financial statements, Clifton Gunderson 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 Clifton Gunderson's evaluation are included in this report.

Site Selections

In selecting VA facilities for testing, the assessment teams considered the geographic region, size, and complexity of each hosting facility, as well as the criticality of systems hosted at the facility. Ernst & Young and Clifton Gunderson LLP assessed mission-critical systems at the following locations:

b3, b7(E)

b3, b7(E)

Vulnerability assessment procedures utilized 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 workstations residing on the network infrastructure, databases hosting major applications, Web application servers providing Internet and intranet services, and network devices, including wireless connections.

Compliance with Government Audit Standards

The FISMA assessment 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 March through November 2010. 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 C Assistant Secretary for Information and Technology Comments

Department of Veterans Affairs **Memorandum**

Date: April 11, 2011

From: Assistant Secretary for Information and Technology (005)

Subj: Draft Report: Federal Information Security Management Act Assessment for 2010 (VAIQ # 7084384)

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

1. Thank you for the opportunity to review the subject report. Attached please find our response which details the progress that the Department of Veterans Affairs (VA) has made in implementing the provisions of the Federal Information Security Management Act (FISMA).

2. During FY 2010, VA continued to make progress in improving the effectiveness of its information security program by further defining agency-wide security objectives through issuance of additional policy directives and procedure handbooks. Additionally, VA continued improving system security controls by implementing technological solutions such as remote access, portable storage device encryption, and its "Visibility to the Desktop[redacted]" initiative. This initiative allows central monitoring of all end user computers connected to the network, both local and remote, giving VA the ability to check endpoints for viruses and malware and verifying that the latest security updates are installed. BigFix also has the unique ability to provide visibility to and manage systems connected to the VA network via [redacted] Virtual Private Network. This way, systems that rarely touch the network directly can be managed. b3, b7(E)

3. We appreciate your time and attention to our information security program. If you have questions, please have a member of your staff contact Ruth Cannatti, Acting Deputy ADAS for Cyber Security (005R2), at 202-461-6410.

(original signed by:)

Roger W Baker

Attachment

Response to FY 2010 Office of Inspector General (OIG) Draft Federal Information Security Management Act (FISMA) Assessment (VAIQ #7084384)

1. 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. (This is a modified repeat recommendation from last year.)

Office of Information and Technology Response: Concur. The FISMA Challenge Team, established in 2010, will be addressing this by prioritizing plans of actions and milestones (POA&Ms) by risk level and then proposing a solution to each either through remediation or filing of a waiver as a result of a risk/benefit analysis. Solutions will be established in conjunction with the Deputy Assistant Secretary (DAS) for Information Security and other oversight bodies and will documented in the [redacted]. Multidisciplinary teams will be established from across the enterprise to determine solutions and prepare a consolidated cost estimate for the highest priority tasks which will be included in the capital planning process. b3, b7(E)

2. We recommend the Assistant Secretary for Information and Technology implement control mechanisms to ensure sufficient supporting documentation is captured in the [redacted] to justify Plans of Action and Milestones closures. (This is a repeat recommendation from last year.)

Office of Information and Technology Response: Concur. The FISMA Challenge Team, established in 2010, will be addressing this by prioritizing plans of actions and milestones (POA&Ms) by risk level and then proposing a solution to each either through remediation or filing of a waiver as a result of a risk/benefit analysis. Solutions will be established in conjunction with the Deputy Assistant Secretary (DAS) for Information Security and other oversight bodies and will documented in the [redacted] Multidisciplinary teams will be established from across the enterprise to determine solutions and prepare a consolidated cost estimate for the highest priority tasks which will be included in the capital planning process.

3. We recommend the Assistant Secretary for Information and Technology define and implement clear roles and responsibilities for developing, maintaining, completing, and reporting Plans of Action and Milestones in accordance with Office of Management and Budget Memorandum M-02-01.

Office of Information and Technology Response: Concur. VA procedures specify responsibilities regarding preparation, maintenance, and reporting of POA&Ms. Specifically, VA Handbook 6500.3 (Certification and Accreditation of VA Information Systems), paragraph 4k, assigns systems owners the responsibility for creating and maintaining POA&Ms;

however, Appendix D of VA Handbook 6500 (Information Security Program) makes it a group effort (local chief information officers, information security officers, and system owners) for performing POA&M functions.

The Assistant Secretary for Information and Technology, in collaboration with the DAS for Information Security and Deputy Chief Information Officer for IT Operations, will publish a memorandum standardizing roles and responsibilities for the preparation, maintenance, and closure of POA&Ms. This memorandum will be incorporated into the updated VA Handbook 6500 and next iteration of VA Handbook 6500.3. The target date for publishing this memo will be provided at a later date.

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

Office of Information and Technology Response: Concur. The Assistant Secretary for Information and Technology will include, in the memo mentioned in the response to recommendation 3 above, mechanisms to ensure that POA&Ms are updated to reflect the current status of remediation actions. Currently, the Office of IT Oversight and Compliance (ITOC) validates the closure of POA&Ms as part of its facility assessment reviews.

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

Office of Information and Technology Response: Concur. An enterprise wide solution has been implemented where the [redacted] and server common controls will remediate this weakness. The FISMA Challenge Team will work with the Region Directors to develop standardized implementation for the above solution. b3, b7(E)

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

Office of Information and Technology Response: Concur. There is an enterprise wide solution that has been implemented where menu management reviews are conducted every 90 days. Additionally, the software patch needed to segregate duties for the three roles (requester, approver and obligate) in [redacted] has been fully installed at all sites. The software to enforce the fourth role (certifier/approver) is in the programming phase but on schedule and is expected to be implemented by June 2011. These two software fixes should remediate segregation of duties issues within [redacted]

7. We recommend the Assistant Secretary for Information and Technology enable system audit logs and conduct centralized reviews of security violations on mission-critical systems. (This is a modified repeat recommendation from last year.)

Office of Information and Technology Response: Concur. There is an enterprise wide solution that has been implemented where the [redacted] and server common controls will remediate this issue.

In addition, the Office of Information and Technology will continue to pursue implementation of a software solution, such as Enterprise Log Manager, for information security officers. This will be used for server audit logs only. The kick-off for this application is mid-March 2011 and there has not been an implementation date set yet.

The FISMA Challenge Team will work with the Region Directors and Field Security Officers to develop a standardized implementation solution that will address the workstation audit log review issue. b3, b7(E)

8. We recommend the Assistant Secretary for Information and Technology implement mechanisms to ensure all remote access computers have updated security patches and antivirus definitions prior to connecting to VA information systems.

Office of Information and Technology Response: Concur. [redacted] is being implemented enterprise wide with an implementation date of June 2011. In addition, with the elimination of the [redacted] Citrix Access Gateways (CAGs) are being stood up that with provide a secure opportunity for remote users to continue to execute their business functions.

VA's Network and Security Operations Center (VA-NSOC) maintains the termination points for remote computers and is not authorized to push patches. For Government Furnished Equipment, if the endpoint does not have (1) Guardian Edge, (2) Anti-Virus, or (3) Host Intrusion Prevention System, access is denied; there is no check for compliance on patch status.

The FISMA Challenge Team work with the Region Directors and Field Security Officers to develop a standardized implementation solution that will ensure that oversight and compliance processes are developed, implemented, and tested.

9. We recommend the Assistant Secretary for Information and Technology implement effective Virtual Local Area Network controls to eliminate unauthorized access to sensitive network segments. (This is a modified repeat recommendation from last year.)

Office of Information and Technology Response: Concur. To remediate this weakness, there was an enterprise-wide solution that has been implemented, with phase I completed on September 30, 2010.

The FISMA Challenge Team will work with the Region Directors and Field Security Officers to ensure that standardized oversight and compliance processes are developed, implemented and tested.

10. We recommend the Assistant Secretary for Information and Technology implement automated mechanisms to continuously identify and remediate security weaknesses on VA's network infrastructure, database platforms, and Web application servers. (This is a repeat recommendation from last year.)

Office of Information and Technology Response: Concur. The FISMA Challenge Team will work with the Region Directors and Field Security Officers to develop a standardized implementation solution.

11. We recommend the Assistant Secretary for Information and Technology implement a patch and vulnerability management program to address security weaknesses identified during our assessments of VA's Web applications, database platforms, and network infrastructure. (This is a modified repeat recommendation from last year.)

Office of Information and Technology Response: Concur. There are a number of region wide solutions that have been implemented where utilities such as [redacted] b3, b7(E) address workstations. Servers will be included in FY 2011. There are a number of region wide solutions that have been implemented where utilities such [redacted] and [redacted] remediate security weaknesses when found.

12. We recommend the Assistant Secretary for Information and Technology develop and implement standard security configuration baselines for all VA operating systems, databases, applications, and network devices. (This is a modified repeat recommendation from last year.)

Office of Information and Technology Response: Concur. Currently, Gold Image Operating System Deployment (OSD) and laptop baselines are used enterprise-wide. Server 2008 hardening guidelines, published by Core Systems, are also used. Switch and router configuration baselines and standards need to be developed by Region Directors and Field Security Officers.

13. We recommend the 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.)

Office of Information and Technology Response: Concur. The Office of Information and Technology (OI&T) has established processes that define actions to be conducted to ensure IT solutions are compliant with security requirements. OI&T is still in the process of implementing an audit program to review compliance.

OI&T has established a program to define procedures that integrate information security throughout the life cycle of system development and to ensure that those processes are monitored for compliance. Specifically, Product Development (005Q) is responsible to define, document, and publish requirements that address all aspects of IT product development.

In addition to the Performance Measurement Accountability System (PMAS) ProPath compliance that is slated to be performed by ITOC, there are multiple formal reviews defined within ProPath that are to be performed by the Integrated Project Team. ITOC, an independent organization within OI&T, provides program and facility reviews, including compliance assessments of projects under PMAS. ITOC staff work collaboratively with VA administrations and staff offices to proactively identify weaknesses, improve their processes, and eliminate significant vulnerabilities.

There are also multiple milestone reviews before transition to Independent Verification & Validation (IV&V), Operational Readiness Testing (ORT), and the Integrated Operations Center (IOC), that are supposed to look for a multitude of documentation.

Finally, for some time, Process Management, within Architecture, Strategy, and Design (005E), had Process Quality Gate reviews in several processes for which project teams were supposed to self-report. These were removed last release but are expected to be added back in.

OI&T Product Development (005Q) has established its software development processes in the ProPath repository. This repository is used by all projects and outlines the specific actions, tools, and methods to be used throughout the software development Iifecycle. Security and privacy requirements are specifically enumerated as actions throughout the software development Iifecycle.

Currently, change control is maturing in each region. In order to comply with VA 6500, App D (CM-3), that states processes must be in place, change control boards have been established. These boards review change requests. Service desk applications are being used to annotate system changes and are tracked, monitored, and reported on a timely basis.

ITOC will begin review of its first projects in March 2011 and, based on the outcome, will establish a structured program to implement program-wide.

14. We recommend that the Assistant Secretary for Information and Technology implement processes to ensure information system contingency plans are updated with the required information, plans are fully tested at alternate processing facilities, and lessons learned are communicated to senior management. (This is a modified repeat recommendation from last year.)

Office of Information and Technology Response: Concur. There is currently a Contingency Plan (CP) Template that is use. Annual self reporting of CP tests are conducted and uploaded to [redacted] RO has been implemented enterprise-wide for continuity of operations and availability of critical information. In addition, a new after action report process is being implemented so senior management and required staff will be able to review the actions taken and lessons learned in a standard format. b3, b7(E)

15. We recommend the Assistant Secretary for Information and Technology implement technological solutions to monitor security for all systems interconnections and

network segments supporting VA programs and operations. (This is a repeat recommendation from last year.)

Office of Information and Technology Response: Concur. OI&T is aggressively implementing visibility to all aspects of the Enterprise Network. The following has been achieved in the past 12 months: (1) visibility to all desktop computers, (2) visibility into Regional and Veterans Integrated Service Networks and (3) isolation of medical devices into a segmented Virtual Local Area Network. Next steps are to have visibility to all servers, laptops, and network devices down to the switch level. Once VA-NSOC possesses this visibility, monitoring and analysis will allow the identification of these interconnections and once documented, allow them to be brought into compliance and routed through authorized network connections.

VA Directive 6513 (Secure External Connections) requires monitoring of all systems interconnected. The VA NSOC conducts timely scans and provides support and assistance with remediation. These scans are also used in system assessments.

16. We recommend the Assistant Secretary for Information and Technology identify all external network connections and ensure appropriate Interconnection Security Agreements and Memoranda of Understanding are in place to govern them. (This is a repeat recommendation from last year.)

Office of Information and Technology Response: Concur. VA Directive 6513 (Secure External Connections) requires that documentation be created and added to [redacted] to reflect external network connections. The VA NSOC scans are able to detect unauthorized connections. The FISMA Challenge Team will work with Field Security Officers and Region Directors to develop a standardized implementation solution that will ensure that oversight and compliance processes are developed, implemented, and tested. b3, b7(E)

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

Office of Information and Technology Response: Concur. There are a number of region wide solutions that have been implemented where utilities such as [redacted] and [redacted] provide statistics for review and improvement purposes. The FISMA Challenge Team and Field Security Officers will work with the Region Directors to develop standardized implementation solutions that will ensure that oversight and compliance processes are developed, implemented, and tested.

18. We recommend that the Assistant Secretary for Information and Technology develop mechanisms to ensure system security plans reflect current operational environments, including accurate inventories of systems, software, database platforms, and system interconnections. (This is a modified repeat recommendation from last year.)

Office of Information and Technology Response: Concur. There is a product that is being tested that will automate and upload the System Security Plan. This tool will be introduced to the field so that testing can be done to ensure that it will resolve validation and reporting requirements. The FISMA Challenge Team and Field Security Officers will work with the Region Directors to develop standardized implementation solutions that will ensure that oversight and compliance processes are developed, implemented and tested.

19. We recommend that the Assistant Secretary for Information and Technology develop mechanisms to ensure system security plans are updated to reflect results of security control and analysis testing, compensating control evaluations, and residual risk-based decisions. (This is a modified repeat recommendation from last year.)

Office of Information and Technology Response: Concur. The FISMA Challenge Team will work with the Field Security Officers and Region Directors to develop standardized implementation solutions that will ensure that oversight and compliance processes are developed, implemented, and tested.

20. We recommend that the Assistant Secretary for Information and Technology implement revised risk assessment processes across the enterprise to effectively identify threats to and vulnerabilities of major applications and general support systems. (This is a modified repeat recommendation from last year.)

Office of Information and Technology Response: Concur. The FISMA Challenge Team will work with the Field Security Officers and Region Directors to develop standardized implementation solutions that will ensure that oversight and compliance processes are developed, implemented, and tested.

21. We recommend that the Assistant Secretary for Information and Technology develop mechanisms to ensure risk assessments accurately reflect the current control environment, compensating control recommendations, and the characteristics of the relevant VA facilities. (This is a repeat recommendation from last year.)

Office of Information and Technology Response: Concur. The FISMA Challenge Team will work with the Field Security Officers and Region Directors to develop standardized implementation solutions that will ensure that oversight and compliance processes are developed, implemented, and tested. b3, b7(E)

22. We recommend that the Assistant Secretary for Information and Technology implement mechanisms to ensure all contractors and other users with VA network access participate in and complete required VA sponsored security awareness training. (This is a modified repeat recommendation from last year.)

Office of Information and Technology Response: Concur. To assure that reports can be provided from the VA [redacted] to monitor whether all VA staff (including contractors, trainees, volunteers, etc.) complete required VA security awareness

training, two solutions (beyond manual data entry) have been identified to facilitate adding user profiles to the VA [redacted] provide a well-defined, bulk upload capability for user profiles and open the VA [redacted] to a managed, self-enrollment capability.

Once these capabilities are available through the VA [redacted], the burden to ensure that profiles for all VA non-employee users are entered and managed in the system belongs to the facilities and offices to which they report. Resistance to entering profiles for these staff members has centered on the lack of resources available to do the necessary manual data entry work and required regular data management. The two recommended solutions relieve the first part of the burden, but once in the VA [redacted], these profiles must be managed by the responsible parties to:

- Ensure the users' compliance with VA training requirements
- Ensure only appropriate non-employee profiles are included in reports
- Maintain VA [redacted] user license limitations.

When all VA user learning profiles are managed through the VA [redacted] reliable and complete compliance and deficiency reports for completion of VA required security awareness training can be generated from that single system. b3, b7(E)

Proposed milestones for delivering VA [redacted] user profile bulk-upload and managed, self-enrollment capabilities are as follows:

- Finalize business requirements for both with primary partners (March 2011)
- Develop bulk-upload and managed self-enrollment capabilities in the VA [redacted] and associated VA applications (April 2011)
- Prepare and communicate policy statement requiring use of VA [redacted], termination of other education tracking systems, and establishing means external to VA [redacted] to verify denominators for specific groups of non- employees (April 2011)
- Develop and deliver training (May June 2011)
- Require VA offices to manage external systems establishing denominators (June 27, 2011)
- Go live with bulk upload and managed self-enrollment tools (June 27, 2011)
- Require facilities and offices to manage/QA non-employee user profiles in VA [redacted] (Ongoing)
- Explore opportunities to interface with other VA systems requiring profile data (Ongoing).

23. We recommend that the Assistant Secretary for Information and Technology identify and ensure personnel with specialized security responsibilities fulfill annual specialized computer security training requirements. (This is a modified repeat recommendation from last year.)

Office of Information and Technology Response: Concur. Additional details on implementation of recommendation 23 will be provided at a later date.

24. We recommend the Assistant Secretary for Information and Technology implement mechanisms for updating the FISMA systems inventory, including interfaces with contractor-managed systems, and annually review the systems inventory for accuracy. (This is a modified repeat recommendation from last year.)

Office of Information and Technology Response: Concur. The [redacted] Working Group meets each week for the expressed purpose of reviewing and updating the FISMA systems inventory, including verifying accuracy. Moreover, contractor-managed systems are currently listed in the inventory and that system list is also verified annually. The [redacted] Working Group was chartered in 2007 and has met continually since that time. **Based on the aforementioned actions taken by the [redacted] Working Group, we recommend closure of this recommendation.** b3, b7(E)

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

Office of Information and Technology Response: Concur. IT tracking of software needs to be accomplished by using a portal per region for all Chief Information Officers (CIO) to enter all purchased software and license information. There would be three types, i.e., individual, site, and enterprise. Tracking of the individual licenses will be the responsibility of the facility CIO. The FISMA Challenge Team will work with Field Security Officers, Region Directors, and facility CIOs to develop standardized implementation solutions that will ensure that oversight and compliance processes are developed, implemented, and tested.

26. We recommend that the 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 modified repeat recommendation from last year.)

Office of Information and Technology Response: Concur. Depending on the nature of access, contractor systems are certified and accredited and remote contractor access is managed in the same manner as VA employee access is managed. VA Handbook 6500.6 (Contract Security) has been put into place to make certain that VA contractors meet all the requirements of VA Directive and Handbook 6500 (Information Security) prior to acquisition of the service. The FISMA Challenge Team and Field Security Officers will work together to improve the oversight process to ensure that compliance is met.

Prior Year Recommendations

FY09-13. We recommend that the Assistant Secretary for Information and Technology, in conjunction with the Office of the Secretary and the Office of Public and Intergovernmental Affairs, develop and test continuity of operations plans in accordance with VA Directive and Handbook 0320, Comprehensive Emergency Management Program.

Office of Information and Technology Response: Primary responsibility for the functions called for in this recommendation fall under the Office of Operations, Security, and Preparedness and not the Office of Information and Technology. As such, future recommendations in this area need to be addressed to them.

The Office of Operations, Security, and Preparedness provided the following response: Concur. The Department has recently updated the VA Master Continuity Plan to include all necessary components. Approval and release of the revised VA Master Continuity Plan is scheduled for May 2011.

FY06-03. Review and update all applicable position descriptions to better describe sensitivity ratings, and better document employee personnel records and contractor files to include "Rules of Behavior" instructions, annual privacy, Health Insurance Portability and Accountability Act of 1996 training certifications, and position sensitivity level designations.

Office of Information and Technology Response: The functions called for in this recommendation are not performed by the Office of Information and Technology and need to be addressed in the future by the Office of Operations, Security, and Preparedness/Office of Personnel Security and Identity Management Personnel and Security Suitability Service, cognizant contracting officer representatives, and local Human Resource Offices. Strongly suggest that this recommendation be broken up into individual components and addressed to the cognizant VA organizations. Please also be aware that electronic Rules of Behavior are utilized which users must agree to before continued access is allowed to VA computer- based information systems. b3, b7(E)

The Office of Operations, Security, and Preparedness' Personnel and Security Suitability Service provided the following response: Concur. VA Directive 0710, Personnel Security and Suitability Program, was issued June 4, 2010. This directive requires Human Resources to ensure position risk and sensitivity level designations are periodically reviewed by appropriate officials to ensure designations are up-to-date and consistently applied to all positions. The Directive also requires all Administrations and staff offices to use the Office of Personnel Management's (OPM) [redacted] to designate position risk and sensitivity level for all position descriptions. VA facilities are utilizing the [redacted] for all new position descriptions and will use the tool to update and revise current position descriptions.

Documentation of (1) Rules of Behavior instructions, (2) annual privacy and Health Insurance Portability and Accountability Act of 1996 (HIPPA) training certificates, and (3) position sensitivity designations in employee records and contract files are the responsibility of local Human Resource Officers and cognizant contracting officer representatives.

VA Handbook 0710, Personnel Security and Suitability Program, is in draft and is currently in the process of being updated and revised by the Office of Operations, Security and Preparedness (OSP). OSP is waiting for several regulatory changes to become final from OPM that will have a direct impact on this Handbook. Estimated completion date is October 2011.

The new Handbook will incorporate the final federal regulations covered by Title 5, Code of Federal Regulations, parts 731, Suitability, and 732, National Security Positions. The Handbook will also include the modified Federal Investigative Standards. VA Directive 0710 also requires Human Resources Officers to initiate background investigations on all new employees within the established timeframes. The timeframes will be incorporated into the Handbook, but will be to standards set by OPM and the Intelligence Reform and Terrorism Prevention Act of 2004, as well as 5 CFR, 731 Suitability, which requires investigations be initiated before appointment but no later than 14 days after placement in the position.

FY06-04 Timely request the appropriate levels of background investigations on all applicable VA employees and contractors. Additionally, monitor and ensure timely requests for reinvestigations on all applicable employees and contractors. Monitor the status of the requested investigations.

Office of Information and Technology Response: The functions called for in this recommendation are not performed by the Office of Information and Technology and need to be addressed in the future by the Office of Operations, Security, and Preparedness and the cognizant Human Resources Offices and contracting officer representatives that support the VA organizations/facilities in question.

The Office of Operations, Security, and Preparedness' Personnel and Security Suitability Service provided the following response: Concur. The Personnel Security and Suitability Service (PSS) has been working with VHA and VBA Human Resources Officials to achieve the objective of "[redacted] before Entering on Duty" and training, to this effect, is also taking place in VACO Human Resources. b3, b7(E)

The use of [redacted] is mandated by the Office of Management and Budget (OMB) and OPM pursuant to the E-Government Act of 2002, P.L. 107-347. [redacted] allows applicants to electronically enter, update, and transmit their personal investigative data over a secure Internet connection to their employing agency for review and approval. [redacted] must be used for all investigative types for employees, contractors, affiliates, volunteers and other designated individuals who will need a background investigation.

The Office of Operations, Security, and Preparedness' Security and Investigations Center (SIC) tracks the reinvestigation requirements for employees and notifies the employee when it is time.

VA Directive 0710 requires Human Resources Officers to initiate background investigations on all new employees within the established timeframes. Each organization/facility that initiates background investigations has the ability to monitor the status of the investigative process using the Office of Personnel Management's Personnel Investigations Processing System (PIPS). The timeframes for investigation will be incorporated in the new VA Handbook, 0710 but will be to

standards set by OPM and the Intelligence Reform and Terrorism Prevention Act of 2004, as well as 5 CFR, 731 Suitability, which requires investigations be initiated before appointment but no later than 14 days after placement in the position.

FY06-07 Strengthen physical access controls to correct previously reported physical access control deficiencies, develop consistent standardized physical access control requirements, policies, and guidelines throughout VA, and limit computer room access to individuals with a legitimate need.

Office of Information and Technology Response: **Concur. However, some of the functions called for in this recommendation are not performed by the Office of Information and Technology. Specifically, overall physical security policy and security of VA facilities fall under the Office of Operations, Security, and Preparedness while IT physical security policy and execution fall under the Office of Information and Technology. Strongly suggest that (1) the physical security deficiencies addressed by this recommendation be categorized by responsible organization and (2) recommendations be made to the responsible VA organizations.**

The Office of Operations, Security, and Preparedness provided the following response: Concur. VA Handbook 0730/2 (Security and Law Enforcement) was published on May 27, 2010. This policy guidance provides updated physical access control requirements. The Office of Security and Law Enforcement program inspectors and IT Oversight and Compliance (ITOC) Information Security teams use these policy requirements when assessing facilities.

FY06-08 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. Additionally, ensure the wireless network is segmented and protected from the wired network.

Office of Information and Technology Response: Concur. Additional details on implementation of this recommendation will be provided at a later date.

FY06-09 Identify and deploy solutions to encrypt sensitive data and resolve clear text protocol vulnerabilities.

Office of Information and Technology Response: Concur. Additional details on implementation of this recommendation will be provided at a later date.

FY06-12 Develop and fully implement procedures for protecting sensitive information accessed remotely or removed from VA facilities in accordance with NIST Special Publication 800-53.

Office of Information and Technology Response: Concur. VA Handbook 6500 (Information Security Program) currently provides procedures for protecting sensitive information accessed remotely or removed from VA facilities.

In addition the VA National Rules of Behavior and Contractor Rules of Behavior provide procedures for employees/contractors/students/volunteers for securing sensitive data remotely.

It is anticipated that a new technology for remote access will be in place by July 1, 2011. At that time additional guidance/procedures will be provided to the field regarding its usage.

VA Handbook 6500 is currently being updated to reflect NIST's Special Publication 800-53, Revision 3; any new requirements for remote access will be included in this handbook. Date for final approval of this new handbook is not available at this time.

FY06-13 Complete the implementation of two-factor authentication in accordance with NIST Special Publication 800-53.

Office of Information and Technology Response: Concur. Additional details on implementation of this recommendation will be provided at a later date.

Appendix E OIG Contact and Staff Acknowledgments

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 Katherine Gers Frederick Livingstone Neil Packard Richard Purifoy Gordon Snyder 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