VA Office of Inspector General

OFFICE OF AUDITS & EVALUATIONS

Department of Veterans Affairs

Federal Information Security Management Act Assessment for FY 2011

April 6, 2012
11-00320-138

Department of Veterans Affairs

Memorandum

Date: April 2, 2012

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

Subj: Final Report: *Federal Information Security Management Act Assessment for FY 2011*

To: Assistant Secretary for Information and Technology (005)

1. Enclosed is the final audit report, *Federal Information Security Management Act Assessment for FY 2011* (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 Department of Homeland Security (DHS). DHS uses this data to assist in its oversight responsibilities and 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 2011 consolidated financial statement audit. VA needs to take an agency-wide approach to successfully remediate high-risk issues through its Plans of Action and Milestones; establish effective processes for evaluating information security controls via continuous monitoring and vulnerability assessments; and test the effectiveness of corrective actions for closing recommendations 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 March 28, 2012. The OIG does not express an opinion on the effectiveness of the Department's internal controls during FY 2011. Appendix A presents outstanding recommendations from previous assessments of the Department's information security program from FYs 2006 through 2010. Ernst & Young and the OIG assessed whether the Department's corrective actions successfully addressed the outstanding recommendations in FY 2011.

5. This report provides 31 recommendations, including three 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. The OIG and Ernst & Young determined that six recommendations have been 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 2011 FISMA assessment.

6. Our independent auditors will follow up on all outstanding recommendations and evaluate the adequacy of corrective actions during their FY 2012 FISMA assessment.

Linda A. Halliday

LINDA A. HALLIDAY

Attachment

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

March 28, 2012

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

Dear Mr. Opfer:

Attached is our report on the performance audit we conducted to evaluate the Department of Veterans Affairs' ("VA") compliance with the Federal Information Security Management Act of 2002 ("FISMA") for the federal fiscal year ending September 30, 2011 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 2011 through October 2011. 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 2011.

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

Ernst & Young LLP

ACRONYMS AND ABBREVIATIONS

DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plans of Action and Milestones
SMART	Security Management and Reporting Tool
SQL	Structured Query Language
VistA	Veterans Healthcare Information Systems Technology and Architecture

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)

Report Highlights: VA's Federal Information Security Management Act Assessment for FY 2011

Why We Did This Assessment

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 2011 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 guidelines. We contracted with the independent accounting firms Ernst & Young LLP and Clifton Gunderson LLP to perform the FY 2011 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 risk management program to meet FISMA requirements. While some improvements were noted, FISMA assessments continued to identify significant deficiencies related to access controls, configuration management controls, continuous monitoring controls, and service continuity practices designed to protect mission-critical systems from unauthorized access, alteration, or destruction.

Weaknesses in access and configuration management controls resulted from VA not fully implementing security control standards, including complex password policies on all servers and network devices. Consequently, we identified weak or default user account credentials 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 15,000 outstanding system security risks and corresponding Plans of Action and Milestones to improve its overall information security posture. As a result of the FY 2011 consolidated financial statement audit, Clifton Gunderson LLP concluded a material weakness exists in VA's information security program.

What We Recommend

This report provides 31 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.

Linda A. Halliday

LINDA A. HALLIDAY
Assistant Inspector General
for Audits and Evaluations

TABLE OF CONTENTS

Introduction 1

Results and Recommendations 2

Finding 1 Agency-Wide Risk Management Program 2

Finding 2 Identity Management and Access Controls 5

Finding 3 Configuration Management Controls 7

Finding 4 System Development/Change Management Controls 9

Finding 5 Contingency Planning 10

Finding 6 Incident Response 11

Finding 7 Continuous Monitoring 13

Finding 8 Security Capital Planning 14

Finding 9 Security Awareness Training 15

Finding 10 System Inventory 16

Finding 11 Contractor Systems Oversight 17

Summary Response from the Assistant Secretary for Information and Technology 18

Appendix A Status of Prior Year Recommendations 19

Appendix B Background 25

Appendix C Scope and Methodology 26

Appendix D Assistant Secretary for Information and Technology Comments 28

Appendix E Office of inspector general Contact and Staff Acknowledgments 29

Appendix F Report Distribution 30

INTRODUCTION

Objective

We determined the extent to which VA's information security program and practices comply with Federal Information Security Management Act (FISMA) requirements, Department of Homeland Security (DHS) reporting requirements, and applicable Office of Management and Budget (OMB) and National Institute for Standards and Technology (NIST) guidance. We contracted with the independent accounting firms Ernst & Young LLP and Clifton Gunderson LLP to perform the FY 2011 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 81 major applications and general support systems at 23 VA facilities. The teams identified specific deficiencies in the following areas:

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

This report provides 31 recommendations, including 3 new 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 2011, VA addressed six prior year recommendations; these recommendations are annotated as "closed" in Appendix A.

RESULTS AND RECOMMENDATIONS

Finding 1 Agency-Wide Risk Management Program

FISMA requires each Federal agency to develop, document, and implement an agency-wide information security risk management program. VA has made progress developing policies and procedures as part of its program. However, VA still faces challenges implementing components of its agency-wide information security risk management program to meet FISMA requirements. Consequently, FISMA 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 but Challenges Remain

In 2007, the Department issued VA Directive 6500, *Information Security Program*, and VA Handbook 6500, *Information Security Program*, defining the high-level policies and procedures to support its agency-wide information security risk management program. In FY 2011, VA began updating VA Handbook 6500 to be consistent with revised NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, and to supplement existing VA directives and handbooks. Further, VA devoted considerable resources to identifying information system security risks through its Security Accreditation program. During FY 2011, VA accredited about one-third of its approximately 640 major applications and general support systems, as annually required.

In April 2010, OMB issued Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, comprising FISMA reporting instructions that change the approach in which Federal agencies assess the effectiveness of information security controls and the security posture of information systems. The memo recommends that Federal agencies move toward a risk-based approach to assess system security, using automation tools to gain enterprise awareness through Continuous Monitoring of security controls. To meet these reporting requirements, VA will utilize system security "Authorizations to Operate," and will leverage continuous monitoring mechanisms, such as "Visibility to the Desktop/Server" initiatives to assess system security controls. VA's goal is to move toward near real-time risk management program.

VA has deployed FISMA stakeholder teams to manage the implementation of corrective actions to address recommendations identified in previous FISMA assessments, including consolidation of the Department's Plans of

Action and Milestones (POA&Ms) records. While VA has made progress developing and updating risk management policies and procedures, our FISMA assessments identified deficiencies related to VA's risk management approach, POA&Ms, and system security plans, which are discussed below. Each of these processes are critical for protecting mission-critical systems through appropriate risk mitigation strategies.

Risk Management Strategy

VA has not fully developed and implemented components of its agency-wide information security risk management program to meet FISMA requirements. NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, states that an agency's risk management framework should address "risk from an organizational perspective with the development of a comprehensive governance structure and organization-wide risk management strategy." VA has begun updating its VA Handbook 6500 to provide guidelines on how to comply with revised risk management requirements. Additionally, VA is developing a risk governance structure, including a Risk Management Governance Board and strategy that will monitor system security risks and implement risk mitigation controls across the enterprise. Until this effort is complete, enterprise-wide risks may not be fully identified or mitigated with appropriate risk mitigation strategies.

Plans of Action and Milestones

OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, defines management and reporting requirements for agency POA&Ms, including deficiency descriptions, remediation actions, required resources, and responsible parties. Despite these requirements, assessment teams continue to identify significant deficiencies related to reporting, managing, and closing POA&Ms.

Assessment teams identified numerous POA&Ms that lacked sufficient documentation to justify closure, as well as action items that had missed major milestones and had not been updated to accurately reflect their current status. Further, based on data available from VA's central reporting tool, more than 15,000 outstanding POA&M actions must be taken to remediate risks and improve VA's information security posture. This reporting tool is VA's central database for tracking the number of systems, system security documentation, and relevant remediation activities through POA&Ms. In the prior year, VA reported more than 13,000 oustanding POA&Ms.

POA&M deficiencies were due to a lack of accountability for closing items and a lack of controls to verify supporting documentation had been input to the central database. Unclear responsibility for managing POA&M records defined at the "local" level 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 central database to justify closure of POA&Ms, VA cannot ensure that corresponding security risks have been fully mitigated.

System Security Plans

Assessment teams continue to identify many system security plans with outdated information regarding operational environments, including system interconnection and ownership information. VA Handbook 6500, Appendix D provides guidelines on maintaining and updating system security plans for major applications and general support systems. Because of these deficiencies, system owners may not fully identify relative boundaries, interdependencies, and security risks impacting mission-critical systems.

Recommendations

1. We recommend the Assistant Secretary for Information and Technology fully develop and implement an agency-wide risk management governance structure and strategy along with mechanisms to identify, monitor, and manage risks across the enterprise.
   - This is a new recommendation.
2. 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 repeat recommendation from last year.
3. We recommend the Assistant Secretary for Information and Technology implement mechanisms to ensure sufficient supporting documentation is captured in the central database to justify closure of Plans of Action and Milestones.
   - This is a repeat recommendation from last year.
4. 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.
   - This is a repeat recommendation from last year.
5. We recommend the Assistant Secretary for Information and Technology implement mechanisms to ensure Plans of Action and Milestones are updated to accurately reflect current status information.
   - This is a repeat recommendation from last year.
6. We recommend the Assistant Secretary for Information and Technology develop mechanisms to ensure system security plans reflect current operational environments, including accurate system interconnection and ownership information.
   - This is a modified repeat recommendation from last year.

Finding 2 Identity Management and Access Controls

Assessment teams identified significant deficiencies in VA's identity management and access controls. VA Handbook 6500, Appendixes D and F, provides comprehensive guidelines for authenticating users and protecting VA's critical systems from unauthorized access, alteration, or destruction. However, our FISMA assessment identified significant information security control deficiencies in the following areas:

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

Password Management

While VA Handbook 6500, Appendix F establishes password management standards for authenticating VA system users, our 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 financial systems and servers were not configured to enforce VA's password policy standards.

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

Access Management

VA Handbook 6500, Appendix D details access management policies and procedures for VA's information systems. However, reviews of permission settings identified numerous instances of unnecessary system privileges, unauthorized user accounts, accounts without formal access authorizations, and active accounts for terminated employees. This occurred because VA has not implemented effective reviews to eliminate such instances of unauthorized system access and excessive permissions. Periodic reviews are critical to restrict legitimate users to specific systems, programs, and data and to prevent unauthorized access by both internal and external users. Unauthorized access to critical systems can leave sensitive data vulnerable to inappropriate modification or destruction.

Audit Trails

VA did not consistently review security violations and audit logs supporting mission-critical systems. VA Handbook 6500, Appendix D, provides high-level policy and procedures for collection and review of system audit logs. However, most VA facilities did not have audit policy settings configured on major systems and had not implemented automated mechanisms needed to periodically monitor systems audit logs. Such audit trail reviews are critical to facilitate security-related activities, such as determining individual accountability, reconstructing security events, detecting intruders, and identifying system performance issues.

Remote Access

VA lacks a consistent process for managing remote access to VA networks. VA Handbook 6500, Appendix D, establishes high-level policy and procedures for managing remote connections. VA personnel can remotely log onto VA networks using several virtual private network applications for encrypted remote access. However, one specific application does not ensure end-user computers are updated with current system security patches and antivirus signatures before users remotely connect to VA networks. Although the remote connections are encrypted, end-user computers could be infected with malicious viruses or worms, which can easily spread to interconnected systems. VA is migrating most remote users to virtual private network solutions that will better protect end-user computers through automated system updates. Moving forward, VA needs to ensure that all remote users' computers are adequately protected before connecting to VA networks.

Recommendations

7. 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 repeat recommendation from last year.
8. 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 repeat recommendation from last year.
9. 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 repeat recommendation from last year.
10. 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.
    - This is a repeat recommendation from last year.

Finding 3 Configuration Management Controls

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

Unsecure Web Applications

Assessments of Web-based applications identified several instances of VA data facilities hosting unsecure Web-based services that could allow malicious users to gain unauthorized access to VA information systems. Additionally, an attacker could potentially alter sensitive data or covertly run unauthorized programs on Web applications. NIST Special Publication 800-44, Version 2, *Guidelines in Securing Public Web Servers,* recommends "Organizations should implement appropriate security management practices and controls when maintaining and operating a secure Web Server." This occurred because VA has not implemented effective controls to identify and remediate security weaknesses on its Web applications. VA has mitigated some information system security risks from the Internet through the use of network filtering appliances. However, VA's internal network remains susceptible to attack from malicious users who could exploit vulnerabilities and gain unauthorized access to VA information systems.

Unsecure Database Applications

Database vulnerability assessments identified a significant number of unsecure configuration settings that could allow any database user to gain unauthorized access to critical system information. NIST Special Publication 800-64, Revision 1, *Security Considerations in the Information System Development Life Cycle,* states that configuration management and control procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the information system. VA has not implemented effective controls to identify and remediate security weaknesses on databases hosting mission-critical applications. Unsecure database configuration settings can allow any database user to gain unauthorized access to critical systems information.

Application and System Software Vulnerabilities

Network vulnerability assessments identified a significant number of outdated operating systems and vulnerable third-party applications that could allow unauthorized access to mission-critical systems and data. NIST Special Publication 800-40, Version 2, *Creating a Patch and Vulnerability Management Program,* states an agency's patch and vulnerability management program should be integrated with configuration management to ensure efficiency. VA has not implemented effective controls to identify and remediate security weaknesses associated with outdated third-party applications and operating system software. Deficiencies in the Department’s patch and vulnerability management program could allow malicious users unauthorized access to mission-critical systems and data. By implementing a robust patch and vulnerability management program, VA could effectively remediate vulnerabilities identified in operating systems, databases, applications, and other network devices.

Baseline Security Configurations

VA continues to develop guidelines to define agency-wide security configuration baselines for its major information system components. FISMA Section 3544 requires each agency to establish minimally acceptable system configuration requirements and ensure compliance. However, we noted that common platform security standards and Federal Desktop Core Configurations are not consistently implemented on all VA systems. For example, testing at VA facilities revealed varying levels of compliance (85 to 99 percent) with Federal Desktop Core Configurations standards for end-user systems. Testing also identified numerous network devices not configured to a common security configuration standard, resulting in default network services, excessive permissions, weak administrator passwords, and outdated versions of network operating system. By not implementing agency-wide configuration management standards for major applications and general support systems, VA is placing critical systems at unnecessary risk of unauthorized access, alteration, or destruction.

Recommendations

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

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

Finding 4 System Development/Change Management Controls

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*, also discusses integrating information security controls and privacy throughout the life cycle of each system.

Our assessment teams determined that software changes to mission critical systems and infrastructure network devices did not follow standardized software change control procedures. Further, numerous test plans, test results, and approvals were either incomplete or missing. By not enforcing a standardized change control methodology, system development projects may be inconsistently developed, tested, and migrated into production, placing VA systems at risk of unauthorized or unintended software modifications.

Recommendation

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 contingency plans are not completely documented and tested and test results are not consistently communicated to senior management. While VA Handbook 6500, Appendix D establishes high-level policy and procedures for contingency planning and plan testing, our assessment identified the following deficiencies.

- Many contingency plans lacked required information, such as Business Impact Analysis data, identification of critical IT resources and recovery priorities, and vendor service-level agreements.
- In most cases, contingency plans tested did not appropriately validate whether system owners could restore those systems in the event of actual disruption. Key components of the contingency plans such as the Activation/Notification, Recovery, and Reconstitution phases were not appropriately tested, and test results were not reported to senior management via after-action reviews as required.
- Alternate site recovery strategies were not fully tested for major applications hosted at data centers and other VA facilities. 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 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, including at alternate processing facilities; and lessons learned are communicated to senior management.

    - This is a 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. Assessment teams identified deficiencies with VA's security incident management and external network monitoring processes.

VA performs significant monitoring of its known Internet gateways to identify and respond to computer security events and potential network intrusions. This monitoring includes some event correlation, which is the process of tying multiple monitoring entries together to identify larger trends, intrusions, or intrusion attempts. However, VA has not fully implemented security information and event management technologies needed for effective event correlation analysis.

VA has not established timelines for responding to computer security incidents as recommended in NIST Special Publication 800-61, *Computer Security Incident Handling Guide*. The guide provides example computer security incident response times ranging from 15 minutes to 4 hours, based on criticality of the incident. The guide also recommends that organizations develop their own incident response times based on organizational needs and the criticality of resources impacted by the security incident. Without establishing incident response timelines and resolving security incidents in a timely manner, there is increased risk that other systems could be exposed to viruses and other malicious code already experienced on VA networks.

To improve incident management, VA's Network Security Operations Center continues to implement its Trusted Internet Connection initiative to identify all system interconnections and consolidate them into four VA gateways. Although progress has been made in cataloging the many interconnections for monitoring purposes, unknown connections still exist. In addition, our assessment teams continued to identify several system interconnections without valid Interconnection Security Agreements and Memoranda of Understanding to govern them. Ineffective monitoring of external network interconnections could prevent VA from detecting and responding to an intrusion attempt in a timely manner.

Recommendations

16. We recommend the Assistant Secretary for Information and Technology implement technological solutions, including a security event and incident correlation solution, 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.
18. We recommend the Assistant Secretary for Information and Technology develop and implement agency-wide incident response timelines and ensure the timely resolution of computer security and privacy incidents in accordance with set standards.
    - This is a new recommendation.

Finding 7 Continuous Monitoring

VA lacks a continuous monitoring process to effectively identify its hardware and software inventory and perform automated monitoring for unauthorized software and hardware devices. NIST Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, outlines the importance of deploying automated mechanisms to detect unauthorized components and configurations within agency networks. Because of inadequate VA monitoring procedures, our technical testing continued to identify significant deficiencies with configuration management controls designed to protect mission-critical systems from unauthorized access, alteration, or destruction. For instance, our testing continues to identify 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.

To better meet continuous monitoring requirements, VA is developing a new enterprise-wide continuous monitoring plan based on the Continuous Asset Evaluation, Situational Awareness, and Risk Scoring model. VA is improving systems and data security control protections by implementing technological solutions, such as secure remote access, application filtering, and portable storage device encryption. Further, VA is deploying various software and configuration monitoring tools to VA facilities as part of its “Visibility to Server” and “Visibility to Desktop” initiatives. Nonetheless, our testing reveals that VA facilities have not made effective use of these tools to actively monitor their networks for unauthorized software, hardware devices, and system configurations.

Recommendation

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

Finding 8 Security Capital Planning

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

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

Recommendation

20. We recommend the Assistant Secretary for Information and Technology develop procedures to integrate information security costs into the capital planning process, while ensuring traceability of Plans of Action and Milestones remediation costs to appropriate capital planning budget documents.
    - This is a new recommendation.

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. As a result, our testing identified numerous personnel who had not completed VA's security awareness training at VA facilities. VA Handbook 6500, Appendix D, establishes high-level policy and procedures for the Department's security awareness training program, requiring all users of sensitive information to annually complete VA's security awareness training.

VA utilizes an online training system, to provide user access to a number of online training resources and track required security awareness and other training for VA employees. However, VA relies largely on manual processes for tracking training requirements for residents, volunteers, and contractors, as automated tracking mechanisms have not been developed. Without automated tracking to support centralized monitoring and more accurate reporting, management cannot ensure that these personnel complete the annual security awareness training requirements.

In FY 2011, VA launched a program to identify users in specific information technology job functions and implement appropriate specialized security training within a centralized system; however, this program is not fully implemented. Our testing identified numerous personnel at VA facilities with significant information technology responsibilities who had not completed specialized security training. More specifically, employees such as information technology specialists, system administrators, and database administrators did not complete specialized training in FY 2011. Without centralized tracking of specialized security training requirements, VA lacks assurance that personnel have the skills needed to protect mission-critical systems and data. Computer security awareness training and specialized security training are essential to help employees and contractors understand their information security and privacy responsibilities.

Recommendations

21. We recommend 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 repeat recommendation from last year.
22. We recommend the Assistant Secretary for Information and Technology identify and ensure personnel with specialized security responsibilities fulfill annual specialized computer security training requirements.
    - This is a repeat recommendation from last year.

Finding 10 System Inventory

This year's assessment identified some inaccuracies in VA's inventory of contractor-managed systems and deployed software. FISMA reporting requirements and VA Handbook 6500, Appendix D, define the information systems inventory requirements for the Department, including contractor-managed systems. The Office of Cyber Security maintained its inventory of information systems within a centralized database, used for FISMA reporting purposes. However, the inventory did not identify interfaces between contractor-managed systems and VA internal networks as required by FISMA. Unidentified contractor systems and interfaces could pose significant risks to VA operations if not properly evaluated and mitigated by appropriate compensating controls.

VA uses custom developed applications to inventory hardware at VA facilities. While the Department has deployed software monitoring tools as part of its "Visibility to Server" and "Visibility to Desktop" initiatives, it has not developed the tools necessary to inventory the software components supporting critical programs and operations. Incomplete inventories of critical software components can hinder patch management processes and restoration of critical services in the event of a system disruption or disaster.

Recommendations

23. We recommend the Assistant Secretary for Information and Technology implement mechanisms for updating the Federal Information Security Management Act systems inventory, including interfaces with contractor-managed systems, and annually review the systems inventory for accuracy.
    - This is a repeat recommendation from last year.

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

Finding 11 Contractor Systems Oversight

In FY 2011, VA did not fully implement contractor oversight procedures as required by FISMA. According to FISMA Section 3544, an agency should ensure information security for the systems that support its operations, including those provided by another agency, contractor, or other source. In addition, VA Handbook 6500.6, *Contract Security*, provides detailed guidance on contractor systems oversight and establishing security requirements for all VA contracts involving sensitive VA information. Despite these requirements, our assessment disclosed several deficiencies in VA's contractor oversight activities in FY 2011.

- Three contractor-owned and operated systems were being used without a valid "Authorization to Operate."
- Eight contractor-owned and operated systems had not performed annual contingency plan 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

25. We recommend 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 repeat recommendation from last year.

Summary

Response from the 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 treats the protection of Veteran data very seriously. Accordingly, VA has embarked on a cultural transformation with implementation of the Continuous Readiness in Information Security Program (CRISP). The Assistant Secretary stated that CRISP embodies an integrated approach to protecting sensitive information from inappropriate exposure or loss. CRISP is a Secretarial priority to achieve and sustain continuous readiness in information security VA-wide. We will continue to evaluate VA's progress during our assessment of the Department's information security program in FY 2012.

Appendix A Status of Prior Year Recommendations

Appendix A documents the status of recommendations from our FISMA assessments for FY 2006 through FY 2010. As noted in the table below, some recommendations remain in progress; however, others have been closed because they were superceded by more current recommendations presented in this report. In FY 2011, VA addressed six recommendations, which are denoted as "closed" in the table below. The corrective actions outlined below are based on management assertions and results of our assessment testing.

Number	Recommendation	Status *(In Progress / Closed)*	Estimated Completion	Corrective Actions
FY 2010–09	We recommend the Assistant Secretary for Information and Technology implement effective Virtual Local Area Network controls to eliminate unauthorized access to sensitive network segments.	Closed	Not Applicable	VA has developed and deployed a Medical Device Virtual Local Area Network scheme for all VA Medical Centers.
FY 2010–19	We recommend 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.	Closed See related recommendation FY 2011–06 from this year.	Not Applicable	VA is considering the issuance of an Executive Directive Memorandum to all system owners requiring them to update system security plans to ensure all required components are included in the plans.
FY 2010–20	We recommend 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.	Closed See related recommendation FY 2010–21 from prior year.	Not Applicable	VA is in the process of deploying a Risk Management Governance Board, which will implement uniform risk assessment procedures throughout VA.

Number	Recommendation	Status *(In Progress / Closed)*	Estimated Completion	Corrective Actions
FY 2010–21	We recommend the Assistant Secretary for Information and Technology develop mechanisms to ensure risk assessments accurately reflect the current control environment, compensating control recommendations, and the characteristics of the relevant VA facilities.	In Progress	To Be Determined	VA is in the process of deploying a Risk Management Governance Board, which will implement uniform risk assessment procedures throughout VA.
FY 2009–13	We recommend 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*.	Closed	Not Applicable	VA conducted various tests of continuity of operations plans in FY 2011.
FY 2006–03	We recommend the Assistant Secretary for Information and Technology review and update all applicable position descriptions to better describe sensitivity ratings, and better document employee personnel records and contractor files, including "Rules of Behavior" instructions; annual privacy, Health Insurance Portability and Accountability Act of 1996 training certifications; and position sensitivity level designations.	In Progress	To Be Determined	VA is developing a Service Support Agreement that details the responsibilities of Human Resources for designating categorizations. VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. have not been finalized.

Number	Recommendation	Status *(In Progress / Closed)*	Estimated Completion	Corrective Actions
FY 2006–04	We recommend the Assistant Secretary for Information and Technology request appropriate levels of background investigations be completed for all applicable VA employees and contractors in a timely manner. Additionally, monitor and ensure timely reinvestigations on all applicable employees and contractors. Monitor the status of the requested investigations.	In Progress	To Be Determined	VA established the Security Investigation Center to ensure background investigations are conducted. A procedure has also been established for information/system owners to request from Human Resources or the Security Investigation Center renewal of employee/contractor background investigations. However, exceptions related to timely background investigations continued to be identified during FY 2011 Federal Information System Controls Audit Manual testing.
FY 2006–07	We recommend the Assistant Secretary for Information and Technology 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 legitimate needs.	Closed	Not Applicable	VA updated Handbook 0730, Appendix B, *Physical Security Requirements and Options*, to ensure it complies with current NIST requirements for physical security. The Department has developed a set of standard minimum criteria for physical access controls applicable to all VA facilities.

Number	Recommendation	Status *(In Progress / Closed)*	Estimated Completion	Corrective Actions
FY 2006–08	We recommend the Assistant Secretary for Information and Technology reduce wireless security vulnerabilities by ensuring sites have an effective and up-to-date methodology to protect against the interception of wireless signals and unauthorized access to the network. 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 VA's wireless network from the wired network. In addition, the Department established the National Wireless Infrastructure Team to ensure all authorized wireless access points to the VA network use a standard wireless network configuration. The Team has established procedures for monitoring for unauthorized wireless systems; however, the procedures are yet to be fully implemented. Potential rogue access points continued to be identified during FY 2011 FISMA testing.

Number	Recommendation	Status *(In Progress / Closed)*	Estimated Completion	Corrective Actions
FY 2006–09	We recommend the Assistant Secretary for Information and Technology identify and deploy solutions to encrypt sensitive data and resolve clear text protocol vulnerabilities.	In Progress	To Be Determined	VA is developing and integrating multiple technologies across the enterprise to encrypt sensitive data, both at rest and in transit. The technologies include: • Sanctuary deployment to ensure only encrypted Universal Serial Bus devices are in use. • Deploy laptop and thumb drive encryption. • Deploy Data Transmission / Attachmate to safely host information on the Web. Further, the "Visibility to Desktop" program verifies deployment of the above technologies and allows for the Department to remediate identified deficiencies. Clear text protocol vulnerabilities continued to be identified during our FY 2011 FISMA testing.

Number	Recommendation	Status *(In Progress / Closed)*	Estimated Completion	Corrective Actions
FY 2006–12	We recommend the Assistant Secretary for Information and Technology develop and fully implement procedures for protecting sensitive information accessed remotely or removed from VA facilities in accordance with NIST Special Publication 800-53.	Closed See related recommendation FY 2011–10 for this year.	Not Applicable	VA is in the process of rationalizing the number of users accessing VA networks remotely utilizing a certain virtual private network client. The virtual private network client does not ensure remote devices have the latest patches and antivirus installed before connecting to the VA network.
FY 2006–13	We recommend the Assistant Secretary for Information and Technology complete the implementation of two-factor authentication in accordance with NIST Special Publication 800-53.	In Progress	To Be Determined	VA is in the process of deploying two factor authentication for system administrators.

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 NIST in its 800 series of special publications supporting FISMA implementation, covering significant aspects of the law. In addition, Federal Information Processing Standards have been issued to establish agency baseline security requirements.

DHS provides instructions to Federal agencies and Inspectors Generals for preparing annual FISMA reports. DHS 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, and testing continuity plans. Per DHS 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 LLP and Clifton Gunderson LLP to conduct the annual FISMA assessment for FY 2011. The OIG provided oversight of the contractors’ performance.

Appendix C Scope and Methodology

The 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 81 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 2011 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

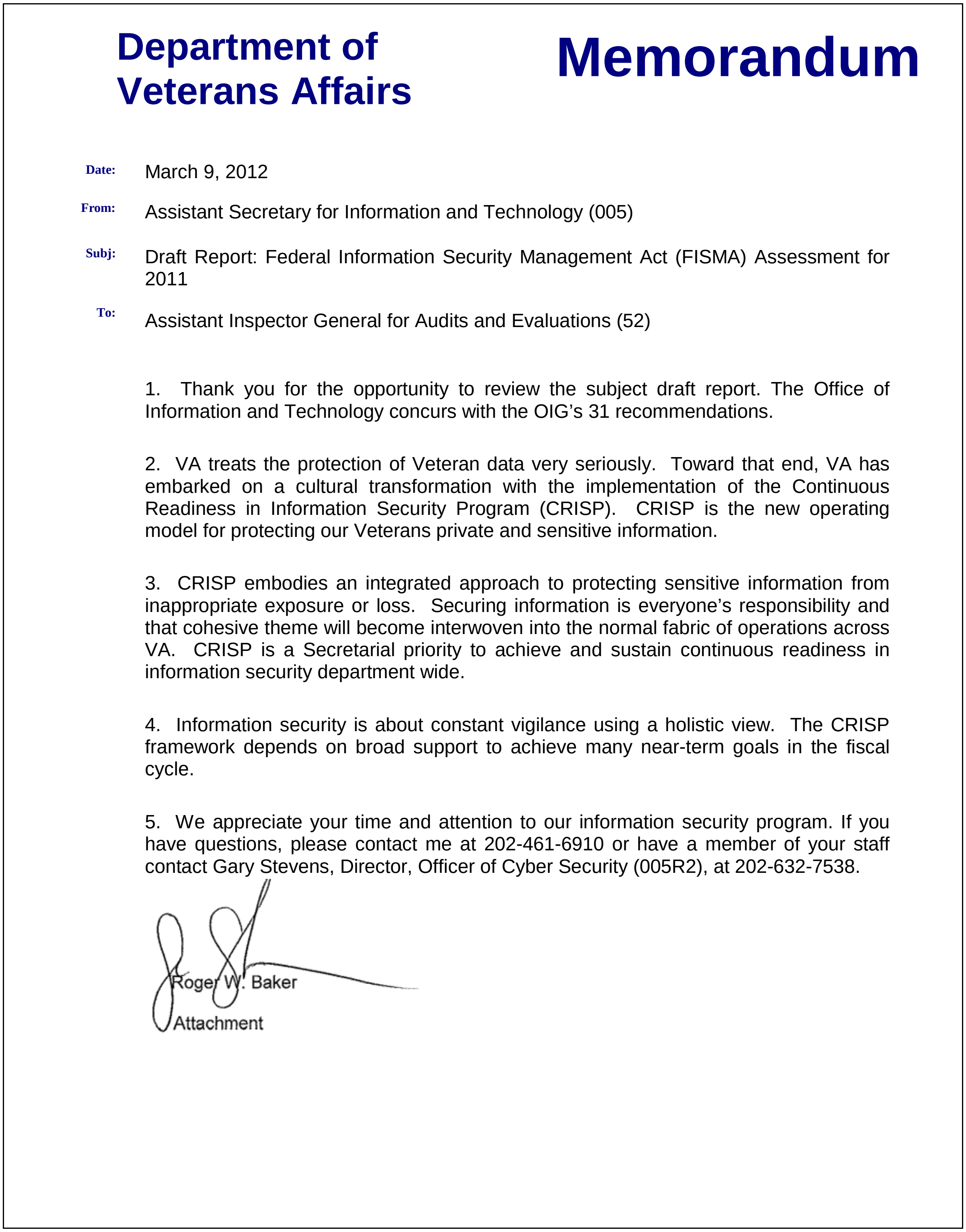
In selecting VA facilities for testing, the assessment teams considered the geographic region, size, and complexity of each hosting facility, as well as the criticality of systems hosted at the facility. Sites selected for testing included: seven major data centers; 11 VA medical facilities; three VA regional offices, one contractor-managed facility; and VA's Central Office located in Washington DC.

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.

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 April through September 2011. Standards for Performance Audits are applicable for this engagement. These standards require the teams plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for findings and conclusions based on the audit objectives. The evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objective.

Appendix D Assistant Secretary for Information and Technology Comments



Department of Veterans Affairs

Memorandum

Date: March 9, 2012

From: Assistant Secretary for Information and Technology (005)

Subj: Draft Report: Federal Information Security Management Act (FISMA) Assessment for 2011

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

1. Thank you for the opportunity to review the subject draft report. The Office of Information and Technology concurs with the OIG's 31 recommendations.

2. VA treats the protection of Veteran data very seriously. Toward that end, VA has embarked on a cultural transformation with the implementation of the Continuous Readiness in Information Security Program (CRISP). CRISP is the new operating model for protecting our Veterans private and sensitive information.

3. CRISP embodies an integrated approach to protecting sensitive information from inappropriate exposure or loss. Securing information is everyone's responsibility and that cohesive theme will become interwoven into the normal fabric of operations across VA. CRISP is a Secretarial priority to achieve and sustain continuous readiness in information security department wide.

4. Information security is about constant vigilance using a holistic view. The CRISP framework depends on broad support to achieve many near-term goals in the fiscal cycle.

5. We appreciate your time and attention to our information security program. If you have questions, please contact me at 202-461-6910 or have a member of your staff contact Gary Stevens, Director, Officer of Cyber Security (005R2), at 202-632-7538.

Roger W. Baker

Attachment

Appendix E Office of Inspector General 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 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
Department of Homeland Security

This report will be available in the near future on the OIG's Web site at http://www.va.gov/oig/publications/reports-list.asp. This report will remain on the OIG Web site for at least 2 fiscal years.