VA Office of Inspector General

OFFICE OF AUDITS AND EVALUATIONS

# Department of Veterans Affairs

*Federal Information Security Modernization Act Audit for Fiscal Year 2016*

**June 21, 2017**
**16-01949-248**

# ACRONYMS

| | |
|---|---|
| CIO | Chief Information Officer |
| DHS | Department of Homeland Security |
| ECST | Enterprise Cybersecurity Strategy Team |
| FISMA | Federal Information Security Modernization Act |
| FY | Fiscal Year |
| GRC | Governance Risk and Compliance |
| NIST | National Institute of Standards and Technology |
| OI&T | Office of Information and Technology |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| POA&M | Plans of Action and Milestones |
| VistA | Veterans Information Systems and Technology Architecture |
| VA | Department of Veterans Affairs |

# Highlights: VA's FISMA Audit for FY 2016

## Why We Did This Audit

The Federal Information Security Modernization Act (FISMA) of 2014 requires agency Inspectors General to annually assess the effectiveness of agency information security programs and practices. Our FY 2016 audit determined whether VA's information security program complied with FISMA requirements and applicable National Institute for Standards and Technology guidelines. We contracted with the independent accounting firm CliftonLarsonAllen LLP to perform this audit.

## What We Found

VA has made progress developing policies and procedures but still faces challenges implementing components of its agency-wide information security continuous monitoring and risk management program to meet FISMA requirements. While some improvements were noted, this audit identified continuing significant deficiencies related to access controls, configuration management controls, continuous monitoring controls, and service continuity practices designed to protect mission-critical systems.

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

Further, VA has not remediated approximately 7,200 outstanding system security risks in its corresponding Plans of Action and Milestones to improve its information security posture. As a result, the FY 2016 Consolidated Financial Statement audit concluded that a material weakness still exists in connection with VA's information security program.

## What We Recommended

This report contains 33 recommendations for improving VA's information security program. We recommended the Acting Assistant Secretary for Information and Technology implement comprehensive measures to mitigate security vulnerabilities affecting VA's mission-critical systems.

## Agency Comments

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

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

# TABLE OF CONTENTS

**DEPARTMENT OF VETERAN AFFAIRS**

# Memorandum

**Date:** June 21, 2017

**From:** Assistant Inspector General for Audits and Evaluations

**Subj:** VA's Federal Information Security Modernization Act Audit for Fiscal Year 2016

**To:** Acting Assistant Secretary for Information and Technology

1. Enclosed is the final audit report, *Federal Information Security Modernization Act Audit for Fiscal Year 2016*. The Office of Inspector General (OIG) contracted with the independent public accounting firm, CliftonLarsonAllen LLP, to assess the Department of Veterans Affairs' (VA) information security program in accordance with the Federal Information Security Modernization Act (FISMA).

2. To ensure the adequacy and effectiveness of information security controls, FISMA requires agency program officials, Chief Information Officers, and Inspectors General to conduct annual reviews of agencies' information security program and report the results to the Department of Homeland Security (DHS). DHS uses these data to assist in its oversight responsibilities and to prepare an annual report to Congress on agency compliance with FISMA.

3. VA continues to face significant challenges in complying with the requirements of FISMA due to the nature and maturity of its information security program. In order to better achieve FISMA outcomes, VA needs to focus on several key areas including specific actions that:

   - Address security-related issues that contributed to the information technology material weakness reported in the FY 2016 audit of VA's Consolidated Financial Statements.
   - Address process deficiencies to ensure that system "Authorizations to Operate" are conducted in accordance with VA policy.
   - Improve deployment of security patches, system upgrades, and system configurations that will mitigate significant security vulnerabilities and enforce a consistent process across all field offices.
   - Improve performance monitoring to ensure controls are operating as intended at all facilities and communicate identified security deficiencies to the appropriate personnel so they can take corrective actions to mitigate significant security risks.

4. CliftonLarsonAllen LLP was contracted to perform the FISMA audit and is responsible for the findings and recommendations included in this report. The OIG does not express an opinion on the effectiveness of VA's internal controls during FY 2016. Our independent auditors will follow up on the outstanding recommendations and evaluate the adequacy of corrective actions during their FY 2017 FISMA audit.

5. This report provides 33 recommendations for improving VA's information security program: 31 recommendations are included in the report body and two recommendations are provided in Appendix A. The appendix addresses the status of prior year recommendations not included in the report body and VA's plans for corrective action. Some recommendations were modified or not closed because relevant security policies and procedures were not finalized or because repeat information security control deficiencies were identified during the FY 2016 FISMA audit. VA successfully closed five recommendations and we identified three new recommendations in FY 2016.

6. The effect of the open recommendations will be considered in the FY 2017 assessment of VA's information security posture. We remain concerned that continuing delays in implementing effective corrective actions to address these open recommendations can potentially contribute to reporting an information technology material weakness for this year's audit of VA's Consolidated Financial Statements.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

CliftonLarsonAllen LLP
www.claconnect.com

May 19, 2017

The Honorable Michael J. Missal
Inspector General
Department of Veterans Affairs
801 I Street, Northwest
Washington, DC 20001

Dear Mr. Missal:

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, 2016 in accordance with guidelines issued by the United States Office of Management and Budget (OMB) and applicable National Institute for Standards and Technology (NIST) information security guidelines.

CliftonLarsonAllen LLP was contracted to perform the FISMA audit and is responsible for the findings and recommendations highlighted in the attached report. We conducted this performance audit in accordance with Government Auditing Standards developed by the Government Accountability Office. This is not an attestation level report as defined under the American Institute of Certified Public Accountants standards for attestation engagements. Our procedures were designed to respond to the FISMA-related questions outlined in the OMB template for the Inspectors General and evaluate VA's information security program's compliance with FISMA requirements and applicable NIST information security guidelines as defined in our audit program. Based on our audit procedures, we conclude that VA continues to face significant challenges meeting the requirements of FISMA.

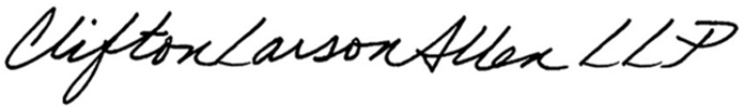
We have performed the FISMA performance audit, using procedures prepared by CliftonLarsonAllen LLP and approved by the Office of the Inspector General (OIG), during the period April 2016 through November 2016. Had other procedures been performed, or other systems subjected to testing, different findings, results, and recommendations might have been provided. The projection of any conclusions, based on our findings, to future periods is subject to the risk that changes made to the information security program or controls, or the failure to make needed changes to the system or controls may alter the validity of such conclusions.

We performed limited reviews of the findings, conclusions, and opinions expressed in this report that were related to the financial statement audit performed by CliftonLarsonAllen LLP. The financial statement audit results have been combined with the FISMA performance audit findings. We do not provide an opinion regarding the results of the financial statement audit results. In addition to the findings and recommendations, our conclusions related to VA are

contained within the OMB FISMA reporting template provided to the OIG in November 2016. The completion of the OMB FISMA reporting template was based on management's assertions and the results of our FISMA test procedures while the OIG determined the status of the prior year recommendations with the support of CliftonLarsonAllen.

This report is intended solely for those on the distribution list on Appendix F, and is not intended to be and should not be used by anyone other than these specified parties.

Sincerely,



CliftonLarsonAllen LLP
Calverton, Maryland
May 19, 2017

# INTRODUCTION

***Objective***

The objective of this audit was to determine the extent to which VA's information security program and practices comply with Federal Information Security Modernization Act (FISMA) requirements, Department of Homeland Security (DHS) reporting requirements, and applicable Office of Management and Budget (OMB) and National Institute for Standards and Technology (NIST) guidance. The VA Office of Inspector General (OIG) contracted with the independent accounting firm CliftonLarsonAllen LLP to perform the FY 2016 FISMA audit.

***Overview***

Information security is a high-risk area Government-wide. Congress passed the Federal Information Security Modernization Act of 2014 (Public Law 113-283) 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. We assessed VA's information security program through inquiries, observations, and tests of selected controls supporting 53 major applications and general support systems at 24 VA facilities. In FY 2016, we identified specific deficiencies in the following areas:

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

This report provides 33 total recommendations, including three new recommendations, for improving VA's information security program. Thirty-one recommendations are included in the report body and two recommendations are provided in Appendix A. The appendix addresses the status of prior recommendations not included in the report body and VA's plans for corrective action. VA successfully closed five recommendations in FY 2016. The FY 2015 FISMA report provided 35 recommendations for improvement.

# RESULTS AND RECOMMENDATIONS

## Finding 1 Agency-Wide Security Management Program

FISMA requires each Federal agency to develop, document, and implement an agency-wide information security and risk management program. VA has made progress developing, documenting, and distributing policies and procedures as part of its program. However, VA still faces challenges implementing components of its agency-wide information security risk management program to meet FISMA requirements. Consequently, this audit identified continuing significant deficiencies related to access controls, configuration management controls, change management controls, and service continuity practices designed to protect mission-critical systems from unauthorized access, alteration, or destruction.

***Progress Made While Challenges Remain***

In FY 2016, the VA's Chief Information Officer formed an Enterprise Cybersecurity Strategy Team (ECST) that developed an enterprise cybersecurity strategic plan. The plan was designed to help VA achieve transparency and accountability while securing veteran information through teamwork and innovation. The team's scope included management of current cybersecurity efforts as well as the development and review of VA's operational requirements from desktop to software to network protection. The ECST has launched 31 Plans of Action to address previously identified security weaknesses and the IT material weakness. The ECST has also reported progress to the Chief Information Officer on a weekly basis to ensure corrective actions are tracked and monitored. As part of the ongoing ECST efforts, we noted continued improvements related to:

- A reduced number of individuals with outdated background investigations
- Use of two-factor authentication to access network resources
- Continued implementation of an IT governance, risk, and compliance tool to improve processes for assessing, authorizing, and monitoring the security posture of VA systems
- Implementation of an enhanced audit log collection and analysis tool

However, these controls require time to mature and demonstrate evidence of their effectiveness. Accordingly, we continue to see information system security deficiencies similar in type and risk level to our findings in prior years and an overall inconsistent implementation of the security program. Moving forward, VA needs to ensure a proven process is in place across the agency. VA also needs to continue to address deficiencies that exist within access and configuration management controls across all facilities. VA has continued to implement the new RiskVision Governance Risk and

Compliance (GRC) tool for the purpose of enterprise wide risk and security management. However, we continue to identify deficiencies related to overall governance and systems authorizations, risk management processes, plans of actions and milestones, system security plans, and privacy impact assessments. Each of these processes is essential for protecting VA's mission-critical systems through appropriate risk mitigation strategies and is discussed in the following sections.

***Governance and Ongoing System Authorizations***

Throughout the FY 2016 FISMA audit, we identified significant issues related to VA's processes for ensuring that system "Authorizations to Operate"[1] were conducted and completed in accordance with the NIST Risk Management Framework and VA policy. Specifically, process deficiencies allowed certain system Authorizations to Operate to expire and allowed other systems to be reauthorized by an official without the proper authority. Furthermore, VA has not implemented processes for conducting security control assessments of medical devices, minor applications, special purpose systems, and industrial control systems before allowing such systems to connect to VA's network or the internet. As a result, Office of Information and Technology (OI&T) has not fully considered the security risks of these systems and devices that were not managed by OI&T but were connected to VA's general network.

***Risk Management Strategy***

VA has not fully developed and implemented components of its agency-wide information security risk management program to meet FISMA requirements. VA has established an enterprise risk management program; however, the policies, procedures, and documentation included in the program were not consistently implemented or applied across all VA systems. For example, Risk Assessments did not consider all known system security risks and threat sources. Specifically, we identified system Risk Assessments that did not address potential external attacks, human error, or previously identified security weaknesses. In addition, we noted that certain risk assessments did not always identify: (a) recommended corrective actions for mitigating security risks, (b) appropriate corrective actions for control weaknesses, or (c) all significant threat sources such as risks associated with devices and systems not managed by OI&T.

NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*: *A Security Life Cycle Approach,* states that an agency's risk management framework should address risk from an organizational perspective with the development of a comprehensive governance structure and an organization-wide risk management strategy. VA has implemented a risk governance structure, including a Risk

[1] System authorization is an official management decision to authorize the operation of an information system and to explicitly accept the system security risks based on the implementation of an agreed-upon set of security controls.

Management Governance Board and the GRC tool, to monitor system security risks and implement risk mitigation controls across the enterprise. However, this effort was not consistently implemented enterprise-wide.

***Plans of Action and Milestones***

OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones* (POA&M), defines management and reporting requirements for agency POA&Ms, to include deficiency descriptions, remediation actions, required resources, and responsible parties. According to VA's central reporting database, the Department had approximately 7,200 open POA&Ms in FY 2016 as compared with 9,000 open POA&Ms in FY 2015. VA dedicated additional resources to work on closing POA&Ms, but much work remains to remediate the significant number of outstanding security weaknesses. POA&Ms identify which actions must be taken to remediate system security risks and improve VA's overall information security posture.

VA has made progress in addressing POA&Ms across VA facilities and systems. Despite these improvements, we continue to identify deficiencies related to reporting, managing, and closing POA&Ms. For example, we identified: (a) POA&Ms that lacked sufficient documentation to justify closure and action items that missed major milestones, (b) POA&Ms that were not reviewed timely or surpassed their scheduled completion dates without justification, and (c) POA&M items that were not updated within the GRC tool to accurately reflect their current status. In addition, we noted that closed POA&Ms within the GRC tool were reopened once a new Authorization to Operate was given to that system. This creates a significant amount of administrative rework when monitoring the current status of valid system risks and also makes it difficult for management to provide an accurate picture of the outstanding system weaknesses due to potential data inaccuracies.

POA&M deficiencies resulted from a lack of accountability for closing items at a "local" level and a lack of controls to ensure supporting documentation was recorded in the GRC Tool. More specifically, unclear responsibility for addressing POA&M records at the local or "regional" level continues to adversely affect remediation efforts across the enterprise. By failing to fully remediate significant system security risks in the near term, VA management cannot ensure that information security controls will adequately protect VA systems throughout their life cycles. Further, without sufficient documentation in the central database to justify closure of POA&Ms, VA cannot ensure that corresponding security risks have been fully mitigated.

***System Security Plans and Privacy Impact Assessments***

We continue to identify system security plans with inaccurate information regarding operational environments, including system interconnections, accreditation boundaries, control providers, and compensating information security controls. We also noted that Privacy Impact Assessments were not consistently updated timely in accordance with policy. Management also did not ensure that the System Security Plans were fully completed, up-to-date, and reflected the current operating environment.

## Recommendations

1. We recommended the Acting Assistant Secretary for Information and Technology implement improved processes to ensure all VA systems and devices are formally "Authorized to Operate" and system security controls are evaluated before allowing such systems to connect to VA's general network or the Internet. *(This is a new recommendation.)*

2. We recommended the Acting Assistant Secretary for Information and Technology fully implement an agency-wide risk management governance structure, along with mechanisms to identify, monitor, and manage risks across the enterprise. *(This is a repeat recommendation from prior years.)*

3. We recommended the Acting Assistant Secretary for Information and Technology implement mechanisms to ensure sufficient supporting documentation is captured to justify closure of Plans of Action and Milestones. *(This is a repeat recommendation from prior years.)*

4. We recommended the Acting Assistant Secretary for Information and Technology implement improved processes to ensure that all identified weakness are incorporated into the Governance Risk and Compliance tool, in a timely manner, and corresponding Plans of Actions and Milestones are developed to track corrective actions and remediation. *(This is a repeat recommendation from prior years.)*

5. We recommended the Acting Assistant Secretary for Information and Technology implement system enhancements to the Governance Risk and Compliance tool to prevent the automatic re-opening of closed Plans of Action and Milestones and such actions are updated to accurately reflect their current status. *(This is a repeat recommendation from prior years.)*

6. We recommended the Acting Assistant Secretary for Information and Technology implement clear roles, responsibilities, and accountability for developing, maintaining, completing, and reporting on Plans of Action and Milestones. *(This is a repeat recommendation from prior years.)*

7. We recommended the Acting Assistant Secretary for Information and Technology develop mechanisms to ensure system security plans reflect current operational environments, including accurate system interconnections, boundary, control, and ownership information. *(This is a repeat recommendation from prior years.)*

8. We recommended the Acting Assistant Secretary for Information and Technology implement improved processes for reviewing and updating key security documents such as risk assessments, privacy impact assessments, and security control assessments on an annual basis and ensure all required information accurately reflects the current environment. *(This is a repeat recommendation from prior years.)*

## Finding 2 Identity Management and Access Controls

We continued to identify significant deficiencies in VA's identity management and access controls. VA Handbook 6500, Appendix F provides comprehensive guidelines for authenticating users and protecting VA's critical systems from unauthorized access, alteration, or destruction. Our FISMA audit identified significant information security control deficiencies in the following areas.

- Password Management
- Access Management
- Audit Logging and Monitoring
- Strong Authentication

***Password Management***

Audit teams continued to identify multiple password management vulnerabilities. For example, we noted weak passwords on major databases, applications, and networking devices at many VA facilities. In addition, password parameter settings for network domains, databases, key financial applications, and servers were not consistently configured to enforce VA's password policy standards. VA Handbook 6500, Appendix F establishes password management standards for authenticating VA system users.

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

***Access Management***

VA has made significant progress in reducing the number of users with elevated privileges on its systems. However, reviews of permission settings still identified numerous instances of unnecessary system privileges, excessive and unauthorized user accounts, accounts without formal access authorizations, and active accounts for terminated personnel. VA Handbook 6500, Appendix F details access management policies and procedures for VA's information systems. Additionally, we noted that user access requests were not consistently reviewed to eliminate conflicting roles and enforce segregation of duties principles.

We also identified inconsistent monitoring of access in production environments for individuals with excessive privileges within certain major applications. This occurred because VA has not implemented effective reviews to monitor for instances of unauthorized system access or excessive permissions. Periodic reviews are critical to restrict legitimate users to specific systems 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 Logging and Monitoring***

VA did not consistently review security violations and audit logs supporting mission-critical systems. VA Handbook 6500, Appendix F provides high-level policy and procedures for collection and review of system audit logs. Specifically, we noted that security logs were not effectively managed or proactively reviewed. For example, platforms such as Veterans Information Systems and Technology Architecture (VistA), databases, and domain controller systems were not included with VA's enhanced audit log monitoring or security event correlation process. In addition, we noted that only failed logon events were collected for windows and infrastructure devices. Collecting only failed logon events increases the risk that successful logons by unauthorized devices or users will not be detected. Audit log reviews are critical for evaluating security-related activities, such as determining individual accountability, reconstructing security events, detecting intruders, and identifying system performance issues. Moreover, we have identified and reported deficiencies with audit logging for more than 10 years in our annual FISMA reports.

***Strong Authentication***

VA has made progress in implementing strong authentication for remote access to its networks. However, we noted that two-factor authentication for local access was not fully implemented across the agency. VA Handbook 6500, Appendix F establishes high-level policy and procedures for managing system connections and authentication standards. Moving forward, VA needs to fully implement strong authentication for all users before connecting to VA networks.

## Recommendations

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

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

11. We recommended the Acting Assistant Secretary for Information and Technology enable system audit logs on all systems and platforms and conduct centralized reviews of security violations across the enterprise. *(This is a modified repeat recommendation from prior years.)*

12. We recommended the Acting Assistant Secretary for Information and Technology fully implement two-factor authentication for all network access methods throughout the agency. *(This is a modified repeat recommendation from prior years.)*

## Finding 3 Configuration Management Controls

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

***Unsecure Web Applications***

Tests 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 onto VA information systems. NIST Special Publication 800-44, Version 2, *Guidelines on Securing Public Web Servers*, recommends that organizations should implement appropriate security management practices and controls when maintaining and operating a secure web server. Despite these guidelines, VA has not implemented effective controls to identify and remediate security weaknesses on its web applications. VA has mitigated some information system security risks from the internet using network-filtering appliances. However, VA's internal network remains susceptible to attack from malicious users who could exploit vulnerabilities and gain unauthorized access to VA information systems.

***Unsecure Database Applications***

Database vulnerability assessments continue to identify a significant number of unsecure configuration settings that could allow any database user to gain excessive unauthorized access permissions to critical system information. NIST Special Publication 800-64, Revision 2, *Security Considerations in the System Development Life Cycle: Information Security*, 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. In addition, key VA financial management systems utilized outdated and unsupported technology that hinders VA's ability to mitigate against certain information security vulnerabilities. Unsecured 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 onto mission-critical systems and data. NIST Special Publication 800-40, Revision 3, *Guide to Enterprise Patch Management Technologies*, states an agency's patch and vulnerability

management program should be integrated with configuration management to ensure efficiency. VA has not implemented effective controls to identify and remediate security weaknesses associated with outdated third-party applications or operating system software. Moreover, we noted that many of VA's legacy systems have been obsolete for several years and are no longer supported by the vendor.

Due to their age, legacy systems are more costly to maintain and difficult to update to meet existing information security requirements. Further, deficiencies in VA's patch and vulnerability management program could allow malicious users to gain unauthorized access into mission-critical systems and data. By implementing a robust patch and vulnerability management program, VA could effectively inventory and remediate vulnerabilities identified in operating systems, databases, applications, and other network devices.

***Unsecure Network Access Controls***

Network vulnerability assessments identified weak network segmentation controls that could allow unauthorized access into mission-critical systems and data. Consequently, VA needs to strengthen its methodologies for monitoring medical devices and ensuring they are properly segregated from other networks. Numerous critical and high-risk vulnerabilities, such as excessive system permissions, were identified residing on unpatched systems and unsecure medical devices that were connected to the general network.

VA did not perform comprehensive scans of all medical devices and other systems connected to VA's network to mitigate security risks posed by these devices. Thus, VA did not have a complete inventory of existing security vulnerabilities on its networks. In addition, OI&T did not manage the configuration and security of certain devices in accordance with VA policy. As a result, our scans identified vulnerabilities that included administrator access to: (1) prescription management software, (2) prescription dispensing robots, and (3) security cameras. We identified a call center recording system that allowed unauthenticated access to all calls since 2013. We identified public-serving kiosks at certain VA medical centers that allowed unauthenticated access to VA's internal network as well as the public Internet.

We noted that several VA organizations shared the same local network at some medical centers and data centers; however, not all systems were under the common control of the local site. Consequently, some networks not controlled by OI&T had significant vulnerabilities that weakened the overall security posture of the local sites. By not implementing effective network segmentation controls for major applications and general support systems, VA is placing other critical systems at unnecessary risk of unauthorized access.

***Baseline Security Configurations***

VA developed guidelines to define agency-wide security configuration baselines for its major information system components. FISMA Section 3544 requires each agency to establish minimally acceptable system configuration requirements and ensure compliance. However, we noted that common platform security standards were not consistently implemented and monitored on all VA platforms. Testing at VA facilities revealed varying levels of compliance, ranging from 89 to 94 percent, when compared to United States Government Configuration Baseline standards.

Testing also identified numerous network devices that were not configured to a common security configuration standard, resulting in default network services, excessive permissions, weak administrator passwords, or outdated versions of system software. Also, VA has not fully documented or approved security baseline standards for all of its systems and platforms and is still working toward approving deviations from the Defense Information System Agency - Standard Technical Implementation Guides that were used to monitor baseline compliance for non-Windows systems. By not implementing consistent agency-wide configuration management standards for major applications and general support systems, VA is placing critical systems at unnecessary risk of unauthorized access, alteration, or destruction.

## Recommendations

13. We recommended the Acting Assistant Secretary for Information and Technology implement more effective automated mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and web application servers. *(This is a repeat recommendation from prior years.)*

14. We recommended the Acting Assistant Secretary for Information and Technology implement a more effective patch and vulnerability management program to address security deficiencies identified during our assessments of VA's web applications, database platforms, network infrastructure, and workstations. *(This is a repeat recommendation from prior years.)*

15. We recommended the Acting Assistant Secretary for Information and Technology maintain complete and accurate baseline configurations and ensure all baselines are appropriately implemented for compliance with established VA security standards. (*This is a modified repeat recommendation from prior years.)*

16. We recommended the Acting Assistant Secretary for Information and Technology implement improved network access controls to ensure medical devices and networks, not managed by the Office of Information and Technology, are appropriately segregated from general networks and

mission-critical systems. (*This is a repeat recommendation from prior years.)*

17. We recommended the Acting Assistant Secretary for Information and Technology consolidate the security responsibilities for networks not managed by the Office of Information and Technology, under a common control for each site and ensure vulnerabilities are remediated in a timely manner. *(This is a repeat recommendation from prior years.)*

18. We recommended the Acting Assistant Secretary for Information and Technology implement improved processes to ensure that all devices and platforms are evaluated using credentialed vulnerability assessments. *(This is a new recommendation.)*

## Finding 4 System Development and Change Management Controls

VA has not fully implemented procedures to enforce standardized system development and change management controls for mission-critical systems. Consequently, we continued to identify software changes to mission-critical systems and infrastructure network devices that did not follow standardized software change control procedures.

FISMA Section 3544 requires establishing policies and procedures to ensure information security is addressed throughout the life cycle of each agency information system. VA Handbook 6500.5, *Incorporating Security and Privacy into the System Development Life Cycle*, also discusses integrating information security controls and privacy throughout the life cycle of each system.

We identified numerous test plans, test results, and approvals that were either incomplete or missing. Specifically, at three major data centers, three VA medical centers, and a contractor facility, we noted that change management policy and procedures for authorizing, testing, and approving system changes were not consistently implemented to support changes to mission-critical applications and networks. By not enforcing a standardized change control methodology, system development projects may be inconsistently developed, tested, and migrated into production, thereby placing VA systems at risk of unauthorized or unintended software modifications.

### Recommendation

19. We recommended the Acting Assistant Secretary for Information and Technology implement improved procedures to enforce a standardized system development and change control framework that integrates information security throughout the life cycle of each system. *(This is a modified repeat recommendation from prior years.)*

## Finding 5 Contingency Planning

VA contingency plans were not fully documented or reflective of current operating environments. VA Handbook 6500, Appendix F establishes high-level policy and procedures for contingency planning and plan testing. Our audit identified the following deficiencies related to contingency planning.

- Certain Information System Contingency Plans did not reflect the current operating environment. Specifically, contingency plans did not clearly identify alternate processing sites, did not contain a complete system inventory or backup procedures, and detailed recovery procedures were not documented in all contingency plans. In addition, contingency plans were not updated to incorporate the lessons learned from contingency plan testing. We identified these issues at nine VA medical centers, two major data centers, and a contractor facility.
- Backup tapes for certain mission-critical systems were not encrypted prior to transporting data offsite for storage. We identified this issue at one major data center and one VA medical center. Overall, we noted an improvement in the encryption of backup data before they were sent offsite compared to the prior year.
- Contingency plans were not tested to ensure failover capability to alternate processing sites. We identified this issue at one major data center, three VA medical centers, and the Health Administration Center.
- The Business Impact Analysis for Financial Management Systems, Personnel and Accounting Integrated Data, and the Veterans Services Network systems did not include the Recovery Point Objectives for each system. These objectives are critical for the planning process to identify the amount of historical data that is acceptable to lose during recovery operations.

Incomplete documentation of contingency and disaster recovery plans may prevent timely restoration of services in the event of system disruption or disaster. Moreover, by not encrypting backup tapes, VA is at risk of potential data theft or unauthorized disclosure of sensitive data. In October 2011, VA implemented the Office of Information and Technology Annual Security Calendar requiring all Information System Contingency and Disaster Recovery Plans to be updated on an annual basis. However, some updated plans continue to have weaknesses similar to those identified in prior years.

### Recommendations

20. We recommended the Acting Assistant Secretary for Information and Technology implement improved processes to ensure information system

contingency plans are updated with the required information. *(This is a modified repeat recommendation from prior years.)*

21. We recommended the Acting Assistant Secretary for Information and Technology implement improved processes for ensuring the encryption of backup data prior to transferring the data offsite for storage. *(This is a modified repeat recommendation from prior years.)*

22. We recommended the Acting Assistant Secretary for Information and Technology implement improved processes for the testing of contingency plans and failover capabilities for critical systems to ensure that all components can be recovered at an alternate site in the event of a system failure or disaster. *(This is a modified repeat recommendation from prior years.)*

23. We recommended the Acting Assistant Secretary for Information and Technology document a Business Impact Analysis for all systems and incorporate applicable Recovery Point Objectives for those systems. *(This is a modified repeat recommendation from prior years.)*

## Finding 6 Incident Response and Monitoring

VA made progress in relation to its overall incident response program, network protection, and monitoring capabilities. Newly implemented technology, additional procedures, and enhanced management awareness have allowed VA to strengthen its incident response and network security program. However, deficiencies were noted in several areas including security event response time, security event correlation, network sensor coverage, vulnerability scan monitoring, and data exfiltration safeguards.

***Some Interconnections Not Monitored***

VA does not monitor all external interconnections and internal network segments for malicious traffic or unauthorized systems access attempts. More specifically, some local facilities had prevented VA's Network and Security Operations Center from periodically testing certain systems for security vulnerabilities. Consequently, VA did not have a complete inventory of all locally hosted systems and must rely on local sites to identify systems for testing. Ineffective monitoring of internal network segments could prevent VA from detecting and responding to intrusion attempts in a timely manner.

Our audit continued to identify numerous high-risk security incidents, including malware infections that were not remediated in a timely manner. Specifically, we noted these issues at three major data centers and two VA medical centers. While VA's performance has improved from the prior year, the process for tracking, updating, and closing security-related incidents was not performed consistently throughout the enterprise. During the year, VA implemented a set of metrics and monitoring procedures to assist with responding to security incidents. The new procedures allowed VA to significantly improve security ticket closure times as the year progressed.

Recently, VA implemented a "Splunk" tool to facilitate enhanced audit log collection and analysis. However, we noted that the tool did not collect data from all systems and platforms. Additionally, VA's Network Security and Operations Center did not have full visibility to evaluate all security-related audit data throughout the enterprise. Management plans to fully implement the "Splunk" tool across all platforms in support of an agency-wide Security Incident and Event Management solution.

***Network Monitoring Needs Improvement***

FISMA Section 3544 requires each agency to develop and implement an agency-wide information security program containing specific procedures for detecting, reporting, and responding to computer security incidents. We performed four unannounced scans of internal networks, and despite Federal requirements for detecting this type of activity, none of these scans were blocked by the Network Security and Operations Center. Management stated that network sensors used to identify suspicious network scanning traffic were not fully implemented throughout the enterprise, resulting in unidentified network vulnerability scanning activity.

VA's ability to detect and prevent data exfiltration through the four Trusted Internet Connection Gateways needs improvement. During testing, we were able to exfiltrate a file that contained mock data including formats resembling social security numbers, email addresses, and passwords through an unencrypted Transmission Control Protocol connection. Thus, VA's perimeter defenses did not block non-standard communication protocols or personally identifiable information traveling outbound to an unknown destination. VA is working on a project to improve gateway monitoring and data exfiltration controls.

## Recommendations

24. We recommended the Acting Assistant Secretary for Information and Technology identify all external network interconnections and implement improved processes for monitoring VA networks, systems, and connections for unauthorized activity. *(This is a repeat recommendation from prior years.)*

25. We recommended the Acting Assistant Secretary for Information and Technology implement more effective agency-wide incident response procedures to ensure timely reporting, updating, and resolution of computer security incidents in accordance with VA standards. (*This is a repeat recommendation from prior years*.)

26. We recommended the Acting Assistant Secretary for Information and Technology ensure that VA's Network Security and Operations Center has full access of all security incident data to facilitate an agency-wide awareness of information security events. *(This is a new recommendation.)*

27. We recommended the Acting Assistant Secretary for Information and Technology implement improved safeguards to identify and prevent unauthorized vulnerability scans and data exfiltrations from VA networks. (*This is a modified repeat recommendation from prior years.*)

## Finding 7 Continuous Monitoring

Although progress has been made, VA lacks a comprehensive continuous monitoring program to manage information security risks and operations across the enterprise. We noted deficiencies related to VA's monitoring of system security controls as well as implementing a consistent standard patch and vulnerability management process to all devices across the enterprise. In addition, an effective agency-wide process was not implemented for identifying and removing unauthorized application software on VA systems. Management is working on improving its enterprise-wide continuous monitoring solution for unauthorized software. We also noted that VA had not fully developed a software inventory to identify applications that support critical programs and operations. NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, outlines the importance of deploying automated mechanisms to detect unauthorized components and configurations within agency networks.

***Inconsistent Security Control Assessments***

VA has incorporated security control assessments within its continuous monitoring program to monitor and manage system security controls. Assessments can be performed by several groups but the primary responsibility for internal security control assessments rests with the local system owner and information security officer. Due to a lack of education and training, the internal control assessment results were inconsistent across the enterprise. Specifically, we identified assessments that did not evaluate the effectiveness of all system operating controls and assessments that did not use sufficient supporting documentation. NIST Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, requires that assessments address the operating effectiveness of controls.

Due to inadequate monitoring procedures, our technical testing continued to identify significant deficiencies with configuration management controls designed to protect mission-critical systems from unauthorized access, alteration, or destruction. For instance, our testing identified unsecured web application servers, excessive permissions on database platforms, a significant number of outdated third-party applications, and inconsistent platform security standards across the enterprise. We also identified devices on networks that were not incorporated into VA's overall vulnerability and patch management process. Specifically, certain devices were not visible to Network Security and Operations Center scanners and system owners did not provide appropriate credentials to allow for comprehensive scanning of vulnerabilities on such devices. Without effectively monitoring device configurations, software, and applications installed on VA networks, malicious users may introduce potentially dangerous software or malware into the VA computing environment.

To better meet continuous monitoring requirements, VA's *Information Security Continuous Monitoring Concept of Operations* established an enterprise information technology framework that supports operational security demands for protection of critical information. This framework is based on guidance from Continuous Monitoring Workgroup activities sponsored by DHS and the Department of State. The Office of Cyber Security continues to develop and implement Continuous Monitoring processes to better protect VA systems. The goal of *Information Security Continuous Monitoring* is to examine the enterprise to develop a real-time analysis of actionable risks that may adversely affect mission-critical systems.

***Software Inventory Processes Need Improvement***

At the time of our audit, VA had improved systems and data security control protections by implementing certain technological solutions, such as the Governance Risk and Compliance (GRC) central monitoring tool, secure remote access, application filtering, and portable storage device encryption. Furthermore, VA had deployed various software and configuration monitoring tools to VA facilities as part of its "Visibility to Server" and "Visibility to Desktop" initiatives. However, VA had not fully implemented the tools necessary to inventory the software components supporting critical programs and operations. Incomplete inventories of critical software components could hinder VA's patch management processes and the restoration of critical services in the event of a system disruption or disaster. Additionally, our testing revealed that VA facilities had not made effective use of these tools to actively monitor their networks for unauthorized software, hardware devices, and system configurations.

## Recommendations

28. We recommended the Acting Assistant Secretary for Information and Technology fully develop a comprehensive list of approved and unapproved software and implement continuous monitoring processes to prevent the use of unauthorized software on agency devices. *(This is a repeat recommendation from prior years.)*

29. We recommended the Acting Assistant Secretary for Information and Technology develop a comprehensive software inventory process to identify major and minor software applications used to support VA programs and operations. *(This is a repeat recommendation from prior years.)*

## Finding 8 Contractor Systems Oversight

VA did not fully implement contractor oversight procedures as required by FISMA. According to FISMA Section 3544, an agency should ensure adequate information security for systems that support its operations, including those provided by another agency, contractor, or other source. In addition, VA Handbook 6500.6, *Contract Security*, provides detailed guidance on contractor systems oversight and establishment of security requirements for all VA contracts involving sensitive VA information. Despite these requirements, our audit disclosed several deficiencies in VA's contractor oversight activities in FY 2016. Specifically:

- VA provided an annual inventory of contractor systems; however, the related system interfaces and interconnection agreements were not included.
- VA did not have adequate controls for monitoring cloud computing systems hosted by external contractors. Consequently, we identified numerous critical and high severity vulnerabilities on contractor networks due to unpatched, outdated operating systems and applications, and configurations not being set to minimize security risks.

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

### Recommendations

30. We recommended the Acting Assistant Secretary for Information and Technology implement procedures for overseeing contractor-managed cloud-based systems and ensure information security controls adequately protect VA sensitive systems and data. *(This is a repeat recommendation from prior years.)*

31. We recommended the Acting Assistant Secretary for Information and Technology implement mechanisms for updating systems inventory, including contractor-managed systems and interfaces, and provide this information in accordance with Federal reporting requirements. *(This is a modified repeat recommendation from prior years.)*

***Management Comments***

The Acting Assistant Secretary for Information and Technology concurred with the findings and recommendations provided in this report and prepared a response, which is presented in Appendix D. In general, management's comments and corrective action plans are responsive to the recommendations and provided sufficient plans and target completion dates. Within the comments, the Acting Assistant Secretary for Information and Technology stated that VA has made progress developing policies and procedures, but

material weaknesses remain in several areas. The Acting Assistant Secretary also stated that VA has created Plans of Action to address the tactical security issues across the enterprise. Further, VA's Enterprise Cybersecurity Strategy Team has created implementation plans across eight domains to further enhance its cybersecurity posture. We will continue to evaluate VA's progress during our audit of VA's information security program in FY 2017. We remain concerned that delays in implementing effective corrective actions to address open recommendations by the estimated completion dates could contribute to the identification of an information technology material weakness during the FY 2017 audit of VA's Consolidated Financial Statements.

# Appendix A Status of Prior-Year Recommendations

Appendix A addresses the status of outstanding recommendations not included in the main report and VA's plans for corrective action. As noted in the table below, two recommendations remain in progress, with estimated completion dates still to be determined. The corrective actions outlined below are based on management assertions and results of our audit testing.

**Table. Status of Prior Year Recommendations**

| Number | Recommendation | Status (In Progress or Closed) | Estimated Completion | Corrective Actions |
|---|---|---|---|---|
| FY 2006–04 | We recommended the Assistant Secretary for Information and Technology ensure appropriate levels of background investigations be completed for all personnel in a timely manner, implement processes to monitor and ensure timely reinvestigations on all applicable employees and contractors, and monitor the status of the requested investigations. | In Progress | December 2017 | VA is implementing an onboarding solution that will establish appropriate business rules based on the position descriptions in order to conduct background investigations and reinvestigations.<br><br>Exceptions related to timely background investigations continued to be identified during FY 2016 FISMA testing. |
| FY 2006–09 | We recommended the Assistant Secretary for Information and Technology identify and deploy solutions to encrypt sensitive data and resolve clear text protocol vulnerabilities. | In Progress | March 2017 | VA has launched a project to encrypt sensitive data transmitted over external and internal data circuits and resolve clear text protocol vulnerabilities.<br><br>Clear text protocol vulnerabilities continued to be identified during our FY 2016 FISMA testing. |

# Appendix B Background

On December 17, 2002, then-President George W. Bush signed FISMA into law, reauthorizing key sections of the Government Information Security Reform Act. The act was amended in December 2014 and became the Federal Information Security Modernization Act. FISMA provides a comprehensive framework for ensuring effective security controls over information resources supporting Federal operations and assets. The statute also provides a mechanism for improved oversight of Federal agency information security programs. FISMA requires each Federal agency to develop, document, and implement an agency-wide security program. VA's security program should protect the information systems that support operations, including those provided or managed by another agency, contractor, or other source. As specified in FISMA, agency heads are responsible for conducting annual evaluations of information security programs and practices.

FISMA also requires agency Inspectors General to assess the effectiveness of agency information security programs and practices. Guidance has been issued by OMB in both circulars and memos and by the National Institute of Standards and Technology (NIST) within its 800 series of special publications supporting FISMA implementation covering significant aspects of the law. In addition, Federal Information Processing Standards have been issued to establish agency baseline security requirements.

OMB and DHS provide instructions to Federal agencies and Inspectors General for preparing annual FISMA reports. In November 2016, OMB issued Memorandum M-17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements*. This memo establishes current information security priorities and provides agencies with FISMA reporting guidance to ensure consistent government-wide performance for protecting national security, privacy, and civil liberties while limiting economic and mission impact of incidents. The memo also provides agencies with quarterly and annual FISMA metrics reporting guidelines that serve two primary functions: (1) to ensure agencies are implementing administration priorities and cybersecurity best practices; and (2) to provide OMB with the data necessary to perform relevant oversight and address risks through an enterprise-wide lens.

The FY 2016 FISMA metrics issued by DHS established minimum and target levels of performance for these priorities, as well as metrics for other key performance areas. To comply with the reporting requirements, agencies must carry out the following activities.

- Chief Information Officers should submit monthly data through CyberScope, the FISMA reporting application. Agencies must upload

data from their automated security management tools into CyberScope on a monthly basis for a specified number of data elements.

- Agencies must respond to security posture questions on a quarterly and annual basis. These questions address areas of risk and are designed to assess the implementation of security capabilities and measure their effectiveness.
- The Chief Information Officers must report to DHS on a quarterly basis, and Inspectors General and Senior Agency Officials for Privacy must report to DHS on an annual basis.
- Agencies must participate in CyberStat accountability sessions and agency interviews conducted by DHS, OMB, and the White House National Security Staff.

DHS reporting instructions also focus on performance metrics related to key control activities, such as continuous monitoring, configuration management, identity and access management, incident response, risk management, security training, plan of action and milestones, contingency planning, and contractor systems. The OIG contracted with the independent accounting firm CliftonLarsonAllen LLP to conduct the annual FISMA audit for FY 2016. The OIG provided oversight of the contractor's performance.

# Appendix C Scope and Methodology

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

This year's work included evaluation of 53 selected major applications and general support systems hosted at 24 VA facilities that support the National Cemetery Administration, the Veterans Benefits Administration, and the Veterans Health Administration lines of business. We 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 2016 Consolidated Financial Statements, CliftonLarsonAllen LLP evaluated general computer and application controls for VA's major financial management systems, following the Government Accountability Office's Federal Information System Controls Audit Manual methodology. Significant financial systems deficiencies identified during CliftonLarsonAllen's evaluation are included in this report.

***Site Selections***

In selecting VA facilities for testing, we 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:

- VA Medical Facility—Augusta, GA
- Information Technology Center—Austin, TX
- VA Medical Facility—Buffalo, NY
- VA Regional Office—Buffalo, NY
- VA Medical Facility—Cleveland, OH
- VA Regional Office—Cleveland, OH
- Terremark, Cloud Service Provider—Culpepper, VA
- VA Health Administration Center—Denver, CO
- VA Medical Facility—Detroit, MI
- Information Technology Center—Hines, IL
- VA Medical Facility—Madison, WI

- Network Security Operations Center—Martinsburg, WV
- Capital Region Readiness Center—Martinsburg, WV
- VA Medical Facility—Northport, NY
- VA Medical Facility—Overton Brooks, LA
- VA Medical Facility—Portland, OR
- VA Medical Facility—Palo Alto, CA
- Information Technology Center—Philadelphia, PA
- VA Insurance Center—Philadelphia, PA
- Loan Guaranty Contractor Managed Facility—Plano, TX
- National Cemetery Administration—Quantico, VA
- VA Medical Facility—Salisbury, NC
- VA Medical Facility—Sioux Falls, SD
- VA Regional Office—Sioux Falls, SD
- VA Central Office—Washington, DC

During site visits, we evaluated 53 mission-critical systems that support VA's core mission, business functions, and financial reporting capability. Vulnerability audit procedures used automated scanning tools and validation procedures to identify high-risk common security vulnerabilities affecting those 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 Standards***

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.

# Appendix D Management Comments

## Department of Veterans Affairs Memorandum

Date: May 12, 2017

From: Acting Assistant Secretary for OI&T and Chief Information Officer (005)

Subj: Draft OIG Report: Federal Information Security Management Act (FISMA) Assessment for FY 2016

To: Assistant Inspector General for Audits and Evaluations

1. VA appreciates the opportunity to respond to the Office Inspector General's (OIG) draft report, *Federal Information Security Management Act Audit for Fiscal Year 2016*. As the OIG's assessment has noted, VA has made progress in developing policies and procedures but material weaknesses remain in several areas.

2. Our efforts will be built upon the progress made in 2016 and 2017; for example:

- In response to the recurring material weakness identified during the FY 2015 OIG FISMA audit, VA created Plans of Action (POA) to address the tactical security issues across the enterprise. Accomplishments within those POAs have been outlined within the recommendation responses.

- As a strategic response, the Enterprise Cybersecurity Strategy Team has created implementation plans across eight domains to further enhance the VA's cybersecurity posture.

3. If you have any questions, feel free to contact me at (202)-461-6910 or feel free to have a member of your staff contact Martha K. Orr, Deputy Chief Information Officer for Quality, Privacy, and Risk (005PR) at (202) 461-6910.

*(original signed by)*

Rob C. Thomas II

Attachment

*For accessibility, the format of the original memo and attachment has been modified to fit in this document.*

Attachment

**Office of Information and Technology**
**Comments to Draft OIG Report,**
**"Federal Information Security Modernization Act Audit for FY 2016"**
**OIG Recommendations and OIT Responses:**

**Recommendation 1:** We recommended the Acting Assistant Secretary for Information and Technology implement improved processes to ensure all VA systems and devices are formally "Authorized to Operate" and system security controls are evaluated before allowing such systems to connect to VA's general network or the Internet. (This is a new recommendation.)

**OI&T Response:** VA concurs with this recommendation. VA has updated the Assessment and Authorization (A&A) process focusing on continuing Risk Management Framework (RMF) initiatives that will aid in monitoring risk and support the organization's mission, business, and operational requirements in accordance with Federal Information Security Modernization Act (FISMA) per the 2014 update, Office of Management and Budget (OMB) Circular A-130, and applicable National Institute of Standards and Technology (NIST) Special Publications [QC Validation FISMA 15-01957-100 Recommendation 1].

Medical devices, special purpose systems, and industrial control systems are part of the Regional General Support System (GSS) accreditation boundary. The devices are captured as part of the Medical Device Protection Program (MPP) – now called the Medical Cyber program. The inventory of these systems was completed on December 31, 2015 and is now being written into the system description of each impacted system security plan at the Regional GSS boundary. Completion of updated System Security Plans (SSPs) and Medical Cyber alignment of systems is expected to be completed by November 30, 2017. If there are identified deficiencies in updating this information or lack of systems identified in the appropriate SSPs, a NIST 800-53 Security Assessment and Authorization (CA) control finding or Plan of Action and Milestone (POA&M) will be opened on the Regional GSS system and tracked through completion.

VA is implementing procedures to address security responsibility for network-connected devices and to assist with the remediation of vulnerabilities. These procedures will assign security responsibilities for network-connected assets under a single authority, obtain inventories of devices, and facilitate security assessments. The inventory and assessment documentation will be added to the governance, risk, and compliance (GRC) tool, where Information Security Officers (ISOs) will analyze compliance with VA policy [NFR IT-2016-10 IT Governance and ATO Process].

In addition, as part of VA's RMF, boundary alignment initiatives are underway to improve the agency's ability to manage and make decisions around security risk in complex environments. VA is working on tasks to monitor and assess accreditation boundaries to confirm compliance with FISMA [NFR IT-2016-01 Information Security Program]. Accomplishments for this recommendation as reported via weekly Enterprise Cybersecurity Strategy Team (ECST) Reporting from December 15, 2015 to March 31, 2017 include:

- Updated A&A policy and process to redefine roles and responsibilities of VA's Authorizing Officials (AO) and AO procedures, which will allow for oversight of systems throughout their full lifecycle [QC Validation FISMA 15-01957-100 Recommendation 1]
- The Enterprise Program Management Office (ePMO) and IT Operations and Services (ITOPS) began preparing and updating the first set of systems to be reconsidered for a new Authorization to Operate (ATO) under the new AO's purview. By the end of calendar year 2016, systems requiring an ATO were updated to reflect the new AO [NFR IT-2016-10 IT Governance and ATO Process].

- Office of Cyber Security Policy and Compliance (OCSPC) conducts routine, regularly scheduled briefings with the AO prior to issuance of ATOs on systems within their purview [NFR IT-2016-10 IT Governance and ATO Process]
- VA has provided ATOs to systems within RiskVision and implemented a measured process to manage expiring ATOs [NFR IT-2016-10 IT Governance and ATO Process, ECST Weekly Accomplishments]
- The Office of Information Security (OIS) is developing draft guidelines on incorporating the business community information owners and project sponsors into the ATO process [NFR IT-2016-10 IT Governance and ATO Process].
- Updated current Security Controls Assessment (SCA) process to meet Federal regulations and evaluate system security controls on an ongoing basis [NFR IT-2016-10 IT Governance and ATO Process]
- Created Case Manager roles to conduct a timely and uniform POA&M process, to determine the level of risk of operation of each information technology (IT) system, and to issue information used to establish a risk determination for VA's AO [NFR IT-2016-10 IT Governance and ATO Process]
- Added existing system inventory to existing GSS (conduct a cybersecurity review) of special purpose systems (SPS) to determine current security posture and appropriate mitigating controls [NFR IT-2016-10 IT Governance and ATO Process]
- Uploaded System Security Plan (SSP) Addendums into the Governance, Risk, and Compliance (GRC) tool (RiskVision) [NFR IT-2016-10 IT Governance and ATO Process] All VA systems have ATO's and system security controls are evaluated before allowing them on the network or internet.

**Target Completion Date:** This project is complete. Request Closure.

**Recommendation 2:** We recommended the Acting Assistant Secretary for Information and Technology fully implement an agency-wide risk management governance structure, along with mechanisms to identify, monitor, and manage risks across the enterprise. (This is a repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. VA has taken steps to implement an agency-wide risk management structure containing a central authoritative information security portal, assess risk-based decisions, provide clear guidelines on cloud and managed service projects to comply with VA security requirements. VA has also updated the A&A process by focusing on increasing system owner accountability to reduce the number of systems with an expired ATO [QC Validation FISMA 15-01957-100 Recommendation 1].

VA focused on continuing RMF initiatives that will aid in monitoring risk and support the organization's mission, business, and operational requirements in accordance with FISMA per the 2014 update, OMB Circular A-130, and applicable NIST Special Publications. Further deployment of A&A procedures will enable VA to confirm Federal regulations are being met [NFR IT-2016-10 IT Governance and ATO Process]. VA Risk Management program is outlined in VA policy and is modeled after NIST requirements. VA specific handbooks and directives for security and RMF include VA Directive 6500 Managing Information Security Risk: VA Information Security Program and VA Handbook 6500 Risk Management Framework for VA Information Systems, VA Information Security Program [QC Validation FISMA 15-01957-100 Recommendation 1].

VA policy is implemented through mandatory employee training (both at the time of initial employment and refreshed annually) provided via the Talent Management System (TMS) and the Certification Program Office (CPO). VA policy is further implemented through SOPs, such as the A&A SOP, which

standardizes business processes of VA's partners, thereby reducing operational risks. VA policy is further implemented through automated Continuous Monitoring (CM) and routine Security Control Assessments [NFR IT-2016-10 IT Governance and ATO Process]. Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to March 31, 2017 include:

- Created a central authoritative VA information security policy portal and assessed current information security policy against Federal requirements
- Assessed and removed existing risk-based decisions (RBDs) for deficiencies, vulnerabilities or risks. Instead, a POA&M process will be used to track identified risks, which aligns to NIST Risk Management guidance
- Enhanced system owner processes that support actions and accountability requirements
- Created the Case Manager role to conduct a timely and uniform POA&M process, determine the level of risk of operation of each IT system, and to issue guidance used to establish a risk determination for VA's AO
- Completed High Value Asset (HVA)-related actions that facilitate the identification, verification, and assessment of security controls of HVAs and sensitive assets
- Formally defined Continuous Monitoring Program with clear lines of authority and responsibility
- Updated A&A process to redefine roles and responsibilities of VA AO and AO procedures, which will allow for oversight of systems throughout their lifecycle
- Updated current SCA process to meet Federal regulations and evaluate system security controls on an ongoing basis
- Created dashboard report to gather metrics on-site performance throughout SCA process, including remediation progress [QC Validation FISMA 15-01957-100 Recommendation 1]

As part of the overall project requirements, task validation was performed by VA's Quality and Compliance (Q&C) Team.

**Target Completion Date: This project was completed on March 31, 2017. Request Closure.**

**Recommendation 3:** We recommended the Acting Assistant Secretary for Information and Technology implement mechanisms to ensure sufficient supporting documentation is captured to justify closure of Plans of Action and Milestones. (This is a repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. VA will further clarify the mechanisms to capture supporting documentation in the central repository to justify closure of POA&Ms, and then implement changes to enhance these functions in an effort to improve execution of the functions, through policy changes and SOPs. In addition, VA will re-train the workforce through mandatory training for primary, secondary, and tertiary roles involved in POA&M management. VA will review existing POA&M workflows inherent within the GRC tool and implement improvements on an as needed basis [NFR IT-2016-05 POA&Ms].

The IG found instances where POA&Ms were not completed in accordance with the scheduled completion date. In the POA&M Management Guide and the training, instructions are provided to the facility on how to update a POA&M when a scheduled completion date was missed. In VA's review, POA&Ms with missed scheduled completion dates were updated in accordance with VA guidelines and training. However, VA will provide further guidance in its training and case material to assist with correctly assigning remediation responsibilities [NFR IT-2016-05 POA&Ms].

VA is in the process of issuing POA&M guidance to describe requirements (including into the Case Manager process), roles and responsibilities, and escalation procedures for noncompliance with RiskVision. Further, VA is enhancing RiskVision functionality and existing training to support the POA&M update process [NFR IT-2016-05 POA&Ms]. Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to April 27, 2017 include:

- Initiated a program to enhance VA's GRC tool functionality and existing training to support the POA&M update process by developing new templates for Privacy Impact Assessments (PIAs), Configuration Management Plans (CMPs), and Contingency Plans (CPs) and training ISOs and system stewards on how to upload artifacts to the GRC tool
- Initiated a program to further define policies and improve training to increase system owner accountability; a related component involves mirroring the Enterprise Operations (EO) instance of the GRC tool to VA Headquarters (HQ) version in a single view, integrating back end databases for EO and HQ versions to include NIST 800-53 Rev. 4 (Privacy) controls, and implementing an improved ticket resolution system
- Deployed specialized technical teams to review POA&Ms, evaluate evidence to support closure, and reviewed each POA&Ms for compliance in accordance with OMB M-02-01
- Implemented Case Manager capability tasked with reviewing POA&Ms and monitoring compliance to allow for elements of a POA&M to be addressed and documented in accordance with OMB M-02-01 and VA Policy
- Released updated Quarterly Action Item (AI) through ITOPS with clear instructions on POA&M review and update requirements to include certification that AI actions are complete
- Established escalation procedures for POA&Ms that are not compliant to include deployment of specialized teams to site, increased oversight and monitoring, and management notification for continued non-compliance [ECST Weekly Accomplishments].

Remaining ECST project activities are scheduled to be completed by December 31, 2017 and include the following tasks:

- Incorporate POA&M requirements into the Case Manager process that will allow POA&Ms to be captured, reviewed, and reported
- Enhance oversight and compliance with the POA&M process
- Enhance GRC training on POA&Ms
- Confirm progress made on POA&M closure in alignment with Case Manager effort.

As part of the overall project requirements, task validation will be performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project is targeted for completion by December 31, 2017.

**Recommendation 4:** We recommended the Acting Assistant Secretary for Information and Technology implement improved processes to ensure that all identified weakness are incorporated into the Governance Risk and Compliance tool, in a timely manner, and corresponding Plans of Actions and Milestones are developed to track corrective actions and remediation. (This is a repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. VA Information Security Program and VA Handbook 6500, Risk Management Framework for VA Information Systems, VA Information Security

Program, provides Guidance for Preparing and Submitting Security Plans of Action and Milestones, defines the process requirements required to determine that identified weaknesses are incorporated into GRC tool, in a timely manner, and corresponding POA&Ms are developed to track corrective actions and remediation. This policy is consistent with OMB Memorandum M-02-01 and NIST requirements. POA&M requirements are implemented via existing SOPs, including the A&A SOP. In addition, VA provides role-based training on these procedures upon initial assignment of the function as well as part of annual refresher training provided by CPO [NFR IT-2016-05 POA&Ms].

Further, VA employs the GRC solution tool to be the singular repository for POA&Ms and this tool is used to manage the POA&M process. Finally, VA implemented dashboard type reporting to monitor overall POA&M status across FISMA systems [NFR IT-2016-05 POA&Ms].VA is in the process of issuing POA&M guidance to clearly describe requirements (including into the Case Manager process), roles and responsibilities, and escalation procedures for noncompliance with RiskVision. Further, VA is enhancing RiskVision functionality and existing training to support the POA&M update process [NFR IT-2016-05 POA&Ms].

Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to April 27, 2017 include:

- Initiated a program to enhance VA's GRC tool functionality and existing training to support the POA&M update process by developing new templates for PIAs, CMPs, and CPs and training ISOs and system stewards on how to upload artifacts to the GRC tool [NFR IT-2016-05 POA&Ms].
- Initiated a program to further define policies and improve training to increase system owner accountability. A related component involves mirroring the EO instance of the GRC tool to VA HQ version in a single view, integrating back end databases for EO and HQ versions to include NIST 800-53 Rev. 4 (Privacy) controls, and implementing an improved ticket resolution system [NFR IT-2016-05 POA&Ms].
- Deployed specialized technical teams to review POA&Ms, evaluate evidence to support closure, and reviewed each POA&M for compliance in accordance with OMB M-02-01[NFR IT-2016-05 POA&Ms].
- Implemented Case Manager capability tasked with reviewing POA&Ms and monitoring compliance to allow for elements of a POA&M to be addressed and documented in accordance with OMB M-02-01 and VA Policy [NFR IT-2016-05 POA&Ms].
- Released updated Quarterly AI through ITOPS with clear instructions on POA&M review and update requirements to include certification that AI actions are complete [NFR IT-2016-05 POA&Ms].
- Established escalation procedures for POA&Ms that are not compliant to include deployment of specialized teams to site, increased oversight and monitoring, and management notification for continued non-compliance [NFR IT-2016-05 POA&Ms].

Remaining ECST project activities are scheduled to be completed by December 31, 2017 and include the following tasks:

- Incorporate POA&M requirements into the Case Manager process that will allow POA&Ms to be captured, reviewed, and reported on
- Enhance oversight and compliance with the POA&M process
- Enhance GRC training on POA&Ms
- Confirm progress made on POA&M closure in alignment with Case Manager effort.

As part of the overall project requirements, task validation will be performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project is targeted for completion by December 31, 2017.

**Recommendation 5:** We recommended the Acting Assistant Secretary for Information and Technology implement system enhancements to the Governance Risk and Compliance tool to prevent the automatic re-opening of closed Plans of Action and Milestones and such actions are updated to accurately reflect their current status. (This is a repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. VA implemented a "HotFix" to the Governance, Risk and Compliance (GRC) Tool. This "HotFix", implemented on September 30, 2016, addresses this recommendation where POA&Ms are re-opened when ATOs are issued [NFR IT-2016-05 POA&Ms]. Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to September 30, 2016 include:

- Tested accuracy of RiskVision dashboard tracking systems undergoing assessments
- Applied the Case Manager construct to additional security artifacts
- Assessed current recommended documentation updates to determine entry by the System Owners (SOs)
- Confirmed that SSPs have completed Facility Compliance Reports to reflect the current environment as part of the Field Security Service (FSS) Security calendar
- Improved RiskVision questionnaire for control implementations that feed SSP control description
- Enhanced RiskVision functionality to support ongoing SSP update process
- Reviewed EO and HQ instances of SSPs, Risk Assessments (RAs), Configuration Management Plans (CMPs) and network diagrams as part of the FSS Security Calendar
- Incorporated SCA results into the SSPs on an ongoing basis.

As part of the overall project requirements, task validation was performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project was completed on September 30, 2016. Request Closure.

**Recommendation 6:** We recommended the Acting Assistant Secretary for Information and Technology implement clear roles, responsibilities, and accountability for developing, maintaining, completing, and reporting on Plans of Action and Milestones. (This is a repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. Existing VA policy, including VA Directive 6500, Managing Information Security Risk: VA Information Security Program and VA Handbook 6500, Risk Management Framework for VA Information Systems, VA Information Security Program, provides Guidance for Preparing and Submitting Security Plans of Action and Milestones, defines roles and responsibilities, management and reporting requirements for agency POA&M, including deficiency descriptions, remediation actions, required resources, and responsible parties. This policy is consistent with OMB Memorandum M-02-01 and NIST requirements [NFR IT-2016-05 POA&Ms].

POA&M requirements are implemented via existing SOPs, including the A&A SOP. In addition, VA provides role-based training on these procedures upon initial assignment of the function as well as part of annual refresher training provided by CPO. Furthermore, VA implemented a singular repository for POA&Ms and this tool is utilized by individuals at many stages of the PO&AM process to store and track

information crucial to managing the POA&M process. Finally, VA implemented dashboard type reporting to monitor overall POA&M status across FISMA systems [NFR IT-2016-05 POA&Ms].

In response to the repeated finding, VA is in the process of issuing POA&M guidance to describe requirements (including into the Case Manager process), roles and responsibilities, and escalation procedures for noncompliance with RiskVision. Further, VA is enhancing RiskVision functionality and existing training to support the POA&M update process [NFR IT-2016-05 POA&Ms]. Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to April 27, 2017 include:

- Issue clarification guidance on POA&M requirements, roles, and responsibilities, escalation procedures, and update process
- Improve accountability for updating POA&Ms
- Confirm GRC solution architecture and remediate issues identified

Remaining ECST project activities are scheduled to be completed by December 31, 2017 and include the following tasks:

- Incorporate POA&M requirements into the Case Manager process that will allow POA&Ms to be captured, reviewed, and reported on
- Enhance oversight and compliance with the POA&M process
- Enhance GRC training on POA&Ms
- Confirm progress made on POA&M closure in alignment with Case Manager effort.

As part of the overall project requirements, task validation will be performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project is targeted for completion by December 31, 2017.

**Recommendation 7:** We recommended the Acting Assistant Secretary for Information and Technology develop mechanisms to ensure system security plans reflect current operational environments, including accurate system interconnections, boundary, control, and ownership information. (This is a repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. VA policy, including VA Directive 6500, Managing Information Security Risk: VA Information Security Program and VA Handbook 6500, Risk Management Framework for VA Information Systems, VA Information Security Program, outlines the requirements for maintaining accreditation related documentation to confirm system security plans reflect current operational environments, including correct system interconnections, boundary, control, and ownership information and these requirements are compatible with NIST requirements. In addition, the GRC tool provides workflows and processes to automate the accreditation documentation development process, with standardized templates, workflows and automatic notifications. Existing VA A&A process workflows are designed to routinely assess accreditation artifacts, including system security plans, risk assessments, privacy impact assessments, and security control assessments during ATO issuance, or at minimum, on an annual basis. These workflows support the risk acceptance process used by the AO to accredit the system [NFR IT-2016-01 Information Security Program].

Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to September 30, 2016 include:

- Tested accuracy of RiskVision dashboard tracking systems undergoing assessments

- Applied the Case Manager construct to additional security artifacts
- Assessed current recommended documentation updates to determine entry by the SOs
- Confirmed that SSPs have completed Facility Compliance Reports to reflect the current environment as part of the FSS Security calendar
- Improved RiskVision questionnaire for control implementations that feed SSP control description
- Enhanced RiskVision functionality to support ongoing SSP update process
- Reviewed EO and HQ instances of SSPs, RAs, CMPs and network diagrams as part of the FSS Security Calendar
- Incorporated SCA Results into the SSPs on an ongoing basis [QC Validation FISMA 15-01957 Recommendation 7,8].

As part of the overall project requirements, task validation was performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project was completed on September 30, 2016. Request Closure.

**Recommendation 8:** We recommended the Acting Assistant Secretary for Information and Technology implement improved processes for reviewing and updating key security documents such as risk assessments, privacy impact assessments, and security control assessments on an annual basis and ensure all required information accurately reflects the current environment. (This is a repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. VA policy, including VA Directive 6500, Managing Information Security Risk: VA Information Security Program and VA Handbook 6500, Risk Management Framework for VA Information Systems, VA Information Security Program, outline the requirements for maintaining, reviewing and updating specific security documents such as risk assessments, privacy impact assessments, and security control assessments and these requirements are compatible with NIST requirements. In addition, the GRC tool, RiskVision, provides workflows and processes to automate the accreditation documentation development process, with standardized templates, workflows and automatic notifications. Existing VA A&A process workflows are designed to routinely assess accreditation artifacts, including system security plans, risk assessments, privacy impact assessments, and security control assessments during ATO issuance, or at minimum, on an annual basis [NFR IT-2016-01 Information Security Program].

As part of the Enterprise Cybersecurity Strategy efforts, OIS will confirm that the System Security Plan templates are updated to enable the inputting of required controls to address NIST SP 800-53, Rev. 4 requirements such as privacy controls (estimated December 2017). VA plans to implement new process changes to enhance current documentation development processes and requirements associated with reviewing and updating specific security documents (e.g., RAs, PIAs, SCAs) are addressed to enhance current procedures and resolve identified gaps. These actions will be leveraged to improve the accuracy of the documentation to more appropriately depict the operational environment of the specific system, while simultaneously driving consistency. Further, VA plans to enhance the current documentation templates within the GRC tool to better support the development of up-to-date, correct documentation [NFR IT-2016-01 Information Security Program].

Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to April 27, 2017 include:

- Train ISOs and System Stewards on security artifact upload (to include PIAs, CMPs, and CPs). Remaining ECST project activities are scheduled to be completed by December 31, 2017 and include the following tasks:

- Perform manual reviews of PIAs, CMPs, and CPs consistent with the security calendar. Identify areas for updating
- Enhance RiskVision functionality to support ongoing, real-time security artifact process Further define policies and increase training to address the system owner understanding of requirements
- Confirm efforts to increase system owner accountability for the security artifact responsibilities
- Confirm effectiveness of updated security artifact process with sample testing.

As part of the overall project requirements, task validation will be performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project is targeted for completion by December 31, 2017.

**Recommendation 9:** We recommended the Acting Assistant Secretary for Information and Technology implement mechanisms to enforce VA password policies and standards on all operating systems, databases, applications, and network devices. (This is a repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. VA has enhanced password monitoring policies via credentialed, predictive scans and remediation processes on OI&T systems. Routine system scans are completed by the Network and Security Operations Center (NSOC). Enterprise Discovery Scans (EDS) are conducted on a quarterly basis to detect password vulnerabilities across the enterprise. In order to improve organization-wide availability of security data, VA has enhanced the reporting of scan results and has published results with historical data on the Nessus Enterprise Web Tool (NEWT). VA is using NEWT dashboards to monitor password vulnerabilities and show trends based on the results of EDS scans. Scan results are shared with users in the enterprise who have been granted access to NEWT [QC Validation FISMA 15-01957-100 Recommendation 10].

A national Flaw Remediation SOP has been developed and published with the intent of strengthening VA's security posture for remediation activities. In addition, password requirements have been added to VA security baselines and a review of security baselines was conducted in September 2016 to identify baselines missing password requirements. Published baselines have been updated to meet the established minimum password requirements [QC Validation FISMA 15-01957-100 Recommendation 10].

VA has implemented Certify to enforce password policies, allowing VA to integrate non-Windows accounts into the Active Directory (AD) to monitor and remediate password vulnerabilities. In an effort to reduce the use of passwords, VA has implemented multi-factor authentication for system administrators. Personal Identity Verification (PIV)-only authentication has made significant progress in implementation across administrations within VA, with exceptions where PIV-only is not technically enforceable. VA has initiated a single sign-on (SSO) program for external (SSOe) and internal (SSOi) users so that applications require passwords in accordance with VA requirements [QC Validation FISMA 15-01957-100 Recommendation 10]. Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to April 27, 2017 include:

- Enhanced quarterly compliance password policy scans
- Established a touchpoint with SSOi and SSOe groups to address application passwords
- Procured and implemented certify for Red Hat Enterprise Linux (RHEL) devices to enforce password policies.

As part of the overall project requirements, task validation was performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project was completed on January 31, 2017. Request Closure.

**Recommendation 10:** We recommended the Acting Assistant Secretary for Information and Technology implement periodic reviews to minimize access by system users with incompatible roles, permissions in excess of required functional responsibilities, and unauthorized accounts. (This is a repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. The VA enhanced privileged access management through development of the Identity, Credential and Access Management (ICAM) Program Management Office (PMO), implementation of the Electronic Permissions Access System (ePAS), and procurement of an automated Privileged Access Management (PAM) solution. The Office of Operations, Security, and Preparedness (OSP) established the ICAM PMO in an effort to help alleviate security deficiencies related to access. The ICAM solution will create an automated process that will tie together the current manual processes for onboarding, monitoring, and off-boarding. The future plans to automate a number of the onboarding, monitoring, and off-boarding process will help VA reach their privileged access management goals for VA Employees, Contractors, Trainees, and Affiliates. Completion of development for ICAM Onboarding solution is projected by end of FY18 [NFR IT-2016-04 Access Request and Periodic Review].

Requests for Elevated Privileges are routed through ePAS. This process requires requestors undergo specialized training as well as receive an electronic hard token for authentication associated with the privileged account. The ePAS system is auditable and requests are to be confirmed by the requestor's supervisor and the ISO [weekly ECST reported accomplishments]. VA has procured an automated PAM solution to serve as an enhancement to the current process. The implementation schedule for the automated solution is currently being developed. The solution will provide additional features, including:

- Password vaulting
- Privileged user session recording
- Privileged service account control
- Random Password management
- Privileged account auto discovery
- Authentication and administration password checkout
- Privileged account analysis and reporting

Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to April 27, 2017 include:

- VA developed an SOP to facilitate the implementation of a manual periodic access review process to track user access to information systems. ISOs, in cooperation with system owners and VA management, manually monitor privileged access so that users have authorization and least privilege to VA information systems. Quarterly reviews are conducted for accounts with Elevated Privileges including both Windows and VistA systems as well as disabled and separated users [NFR IT-2016-04 Access Request and Periodic Review].

As part of the overall project requirements, task validation was performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project was completed on December 31, 2016. Request Closure. Please note enhancement and full implementation of the PAM solution mentioned above are ongoing and will extend into the future.

**Recommendation 11:** We recommended the Acting Assistant Secretary for Information and Technology enable system audit logs on all systems and platforms and conduct centralized reviews of security violations across the enterprise. (This is a modified repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. VA is continuing efforts to enhance the ability to centrally collect and monitor logs and correlate data throughout the enterprise via two primary methods. First, VA's EO team currently collects application related event logs at the National Data Centers using QRadar. Second, NSOC collects mission-critical event logs at the four Trusted Internet Connection (TIC) gateways and other network based infrastructure devices across the enterprise via Splunk Enterprise Security (ES). The implementation of the Splunk ES Security Incident and Event Management (SIEM) solution was completed in November 2016 and included the onboarding of a full-time Splunk subject matter specialist. The national deployment of the Enterprise SIEM (Splunk ES) is now receiving logs from across the enterprise to include centralized logging from devices owned and managed by Field Operations (FO) to include Windows and Linux servers, and network infrastructure devices (routers/switches). Other log sources such as domain controllers, Domain Name Services (DNS), and ePolicy Orchestrator (ePO) systems are now also included in the centralized logging repository, which helps to enrich the data lake and enhance data available for event monitoring, correlation processes and Incident Response. Currently, only failed logon events are being collected for infrastructure devices [NFR IT-2016-08 Security Incidents and Audit Logging].

This expanded Enterprise SIEM capability across VA is a national project using the Splunk ES solution. Capabilities currently available include the ability to review and act on log data from more than 50 mission-critical data feeds (indexes) centrally logged from gateway devices to include log sources in the Capital Region Readiness Center (CRRC) in Martinsburg and the Hines Information Technology Center (ITC) as well as the four TIC gateways. Additionally, the Enterprise SIEM is indexing data from the field that is being received into one of the six regional repositories that have been deployed as part of this initiative [NFR IT-2016-08 Security Incidents and Audit Logging]. The SIEM will continue to be tuned and new data sources added as the NSOC works with EO, Enterprise Systems Engineering (ESE), and FO to develop repeatable sustainable processes for onboarding new data elements as defined in VA Handbook 6500 and Federal standards. Encryption requirements will be addressed by the ECST in ongoing national efforts and plans to encrypt sensitive data at rest. The requirements to encrypt or better protect audit logs will be reviewed for inclusion in the ECST efforts [NFR IT-2016-08 Security Incidents and Audit Logging].

Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to April 27, 2017 include:

- Adopted an enterprise-wide baseline for audit logging to include specified events for Windows gateway indexes and domain controllers
- Performed a wide area network (WAN) capacity analysis on infrastructure services using mission-critical systems (domain controllers) to identify log volumes and allow the NSOC to assess storage and licensing required to incorporate events collected from the enterprise
- Implemented Case Manager capability tasked with reviewing POA&Ms and monitoring
- Completed Splunk ES training at the Hines and Martinsburg locations
- Completed Splunk ES installation and data migration

Remaining ECST project activities are scheduled to be completed by June 30, 2017 and include the following tasks:

- Create a process to review and authorize new data sets onboarded to the SIEM
- Define event management (e.g., monitoring, response to alerts, alert mitigations, etc.) processes across the enterprise.

As part of the overall project requirements, task validation will be performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project is targeted for completion by June 30, 2017.

**Recommendation 12:** We recommended the Acting Assistant Secretary for Information and Technology fully implement two-factor authentication for all network access methods throughout the agency. (This is a modified repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. In response to the Material Weakness identified during the FY15 OIG FISMA audit, VA created a project to address the tactical security issue outlined above. Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to December 31, 2016 include:

- Enforce two-factor authentication (2FA) for both mechanisms used to remotely access VA's network: Remote Enterprise Security Compliant Update Environment (RESCUE) Virtual Private Network (VPN) and Citrix Access Gateway (CAG)
- Users are required to use their PIV card to authenticate at the gateway
- There is a process in place for the National Service Desk (NSD) to provide a temporary exemption from two-factor authentication in emergency situations [NFR-IT-2016-07 Password Standards].

As part of the overall project requirements, task validation was performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project was completed on December 31, 2016. Request Closure.

**Recommendation 13:** We recommended the Acting Assistant Secretary for Information and Technology implement more effective automated mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and Web application servers. (This is a repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. VA has an enterprise-wide scanning program performed by the NSOC on a scheduled and ad-hoc basis (when needed or requested). Results of the scans are rolled into NEWT for analysis and reporting. The analysis tool provides an enterprise view to the terminal device level (specific Internet Protocol [IP]). NEWT coverage has been expanded to include Cisco and Red Hat Enterprise Linux scan results as well as trending and historical remediation efforts. VA implemented DbProtect, a database scanning tool, to gain enterprise level access and insight to the many databases that exist in the organization [NFR IT-2016-09 Vulnerability Configuration Management].

Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to April 27, 2017 include:

- Improved metrics on critical vulnerabilities
- Maintained a master list of vulnerability scan types and frequencies
- Implemented monthly Cisco network device compliance scanning
- Implemented monthly RHEL credentialed vulnerability scanning
- Expanded NEWT vulnerability scan results dashboard to include operating systems/devices scanned
- Expanded vulnerability scanning NEWT health assessment dashboard (which provides month-to-month data vulnerability scans) to include operating systems / devices that are scanned.

Remaining ECST project activities are scheduled to be completed by June 30, 2017 and include the following tasks:

- Enhance NEWT to capture documentation of remediation performed
- Implement a Patch and Vulnerability Management Program. As part of the overall project requirements, task validation will be performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project is targeted for completion by June 30, 2017.

**Recommendation 14:** We recommended the Acting Assistant Secretary for Information and Technology implement a more effective patch and vulnerability management program to address security deficiencies identified during our assessments of VA's Web applications, database platforms, network infrastructure, and workstations. (This is a repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. VA makes use of a number of scanning tools to identify security deficiencies, incorporate findings for a remediation warehouse, and create enterprise view to the terminal device level (specific IP). NSOC has implemented DbProtect for database scanning and has implemented credentialed Cisco Red Hat Linux device scanning. Results are being exported into NEWT. NSOC is in the process of implementing credentialed scanning on additional operating systems and devices across the enterprise [NFR IT-2016-09 Vulnerability Configuration Management].

In addition, VA remediated over 36 million vulnerabilities utilizing Nessus monthly scans and enterprise patching with decreased remediation timeframe since May 2015. The Veterans Benefits Management System (VBMS) was also updated, leading to the remediation of 470,000 vulnerabilities [Continuous Readiness in Information Security Program (CRISP) RSS Update, April 14, 2017]. OI&T is standing up an Enterprise-level Patch and Vulnerability Team (PVT) to address patch and vulnerability management. Responsibilities for PVT activities will include analyzing aged vulnerabilities and creating processes to identify asset owners across VA organizations. A national Flaw Remediation SOP has been developed to strengthen patch and vulnerability management across the enterprise and will be used by the PVT [NFR IT-2016-09 Vulnerability Configuration Management].

VA is implementing a process to use the Remediation Effort Entry Form (REEF) within NEWT to capture documentation of vulnerability remediation. This documentation can be shared with RiskVision to catalog remediation efforts for systems in the GRC tool. The NEWT team conducted training on the tool and established a quarterly recurring training schedule [NFR IT-2016-09 Vulnerability Configuration Management]. This project was tracked in tandem with the project outlined in FY16 Recommendation 13.

Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to April 27, 2017 include:

- Improved metrics on critical vulnerabilities
- Maintained a master list of vulnerability scan types and frequencies
- Implemented monthly Cisco network device compliance scanning
- Implemented monthly RHEL credentialed vulnerability scanning
- Expanded NEWT vulnerability scan results dashboard to include operating systems/devices scanned
- Expanded vulnerability scanning NEWT health assessment dashboard (which provides month-to-month data vulnerability scans) to include operating systems/devices that are scanned

Remaining ECST project activities are scheduled to be completed by June 30, 2017 and include the following tasks:

- Enhance NEWT to capture documentation of remediation performed
- Implement a Patch and Vulnerability Management Program.

As part of the overall project requirements, task validation will be performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project is targeted for completion by June 30, 2017.

**Recommendation 15:** We recommended the Acting Assistant Secretary for Information and Technology maintain complete and accurate baseline configurations and ensure all baselines are appropriately implemented for compliance with established VA security standards. (This is a modified repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. VA has a process for baseline development and implementation, which encompasses the following categories: databases, operating systems, and network devices. VA performed a review of systems in the VA System Inventory (VASI) to identify systems where baselines do not exist and established processes to publish and implement new baselines. Baselines published on the Security Management and Analytics (SMA) SharePoint Portal are confirmed as being accepted. Baselines adopted prior to the Systems Engineering Design Review (SEDR) process were accepted following procedures in place at the time of approval. Baselines adopted since the SEDR process have been accepted through SEDR and changes accepted through Change Control [NFR IT-2016-06 Configuration Management].

Erroneous data on the SMA SharePoint site public view misrepresented 43 systems not being fully ratified through the National Change Control Board (NCCB) and the SEDR process and 53 systems missing the proper information security hardening for Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs). The final gap analysis of currently published baselines with DISA STIGs and VA Handbook 6500 has been completed and VA has a total of 65 baselines that have been fully ratified. Only four configuration baselines require adjustments to include missing DISA STIGs. The SMA portal has been reworked to reflect approval and review dates. Automated reports have been developed for 40% of baselines published on the SMA portal to detect the current status of compliance in regards to security configuration settings [NFR IT-2016-06 Configuration Management].

The current SOP is being modified to strengthen the baseline process and include provisions to review and modify baselines according to an established schedule. As of April 27, 2017, the Structured Query Language (SQL) 2012 baseline has been implemented on 90% of systems (according to VA reporting). Deviations from the SQL 2012 baseline have been documented through POA&Ms submitted by the system owners and ISOs, in order to document the risk and track progress of remediation. Baseline compliance is being monitored and reported in the endpoint security and management tool, BigFix, and System Center Configuration Manager (SCCM) following DISA STIGs and United States Government Configuration Baseline (USGCB) settings. Network devices compliance scanning is being implemented using the NESSUS vulnerability scanning tool and following DISA STIGs. Scan data is being sent to VA NEWT and the NSOC Log Analysis Distributed Database Enterprise Reporting (LADDER) product for analysis and remediation. The DbProtect tool has been procured and installed to perform baseline scanning of databases. A manual compliance screening process has been established for baselines where an automated tool does not exist. Collaboration and communication has been improved between SMA and various entities within the organization that develop and own baselines [NFR IT-2016-06 Configuration Management].

Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to April 27, 2017 include:

- Performed one-time review and update of currently published baselines

- Published new baselines according to technologies in use in the field or emerging technologies
- Created a baseline configuration monitoring matrix
- Determined the delta between BigFix and SCCM as the tools for monitoring server and workstation baseline configurations

Remaining ECST project activities are scheduled to be completed by September 30, 2017 and include the following tasks:

- Implement DbProtect tool for database monitoring to include integration with NEWT
- Develop and publish improved SOP for baseline updates
- Enhance existing tool to provide Cisco network device baseline configuration monitoring across VA.

As part of the overall project requirements, task validation will be performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project is targeted for completion by September 30, 2017.

**Recommendation 16:** We recommended the Acting Assistant Secretary for Information and Technology implement improved network access controls to ensure medical devices and networks, not managed by OI&T, are appropriately segregated from general networks and mission-critical systems. (This is a repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. In response to the Material Weakness identified during the FY15 OIG FISMA, VA created a project to address the security issue outlined above. VA has implemented the Medical Device Protection Program (MDPP) and Enterprise Cyber Security Team (ECST) Medical Cyber (MedCyber) Domain. MDPP / MedCyber address the unique security considerations of VA Medical Devices. Additionally, due to the shared risk responsibility that VA has with medical device manufacturers, which is documented in VA's Medical Device Risk Assessment, medical devices are required to be isolated from VA's business network through the implementation of the Medical Device Isolation Architecture (MDIA). This architecture limits the network communication profile to and from the medical device. Since MDIA is a compensating control for the risks of running medical devices, medical devices found outside of MDIA is, by policy, a security incident that is tracked through VA's incident response process.

Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to September 30, 2016 include:

- VA implemented an automated inventory of network-connected medical devices by comparing the Networked Medical Device Database (NMDD) to SolarWinds as well as documenting network-connected medical devices within applicable host GSS security authorization boundaries.
- VA implemented an inventory reconciliation process whereby VHA Biomedical Engineering staff reconcile their enterprise inventory to the automated inventory in 90 day increments.
- VA implemented an enterprise wide change management process for medical device isolation architecture (MDIA) changes with a change advisory board to determine changes to meet MDIA rules.
- Devices connected to VA's network were documented and inventoried in March 2016 in a system security plan addendum that identified the business owner, administrator, and cybersecurity status of the equipment. These documents were added to the GRC tool as security artifacts.

- OI&T has accepted responsibility for devices connected to VA's network through the issuance of policy that required the networked connected devices, tenant networks and medical devices to be accounted for as part of the existing GSS, making the system owner responsible for devices connected to VA's network.
- VA implemented an enterprise-wide change management process, using the NSD ticketing system, for MDIA changes with a change advisory board – to confirm that changes meet the MDIA ruleset. VA also implemented an enterprise remediation standard operating procedure establishing remediation timelines for MDIA changes that are a result of the MDIA Access Control List (ACL) reviews that find security deficiencies in the ACL implementation.
- As of the end of FY16 (September 30, 2016), MDIA infrastructure achieved 97% compliance with the MDIA ruleset according to ACL summary reporting artifacts associated with this project. The remaining 3% of the ACLs had POA&Ms created for tracking and remediation in the GRC tool. The implementations throughout the year of these processes and procedures have allowed VA to increase its program baseline compliance of 90% and achieve 97% compliance on the MDIA implementation. Network access controls that enable mission-critical medical devices are appropriately segregated from the general network [QC Validation FISMA 15-01957-100 Recommendation 18].

As part of the overall project requirements, task validation was performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project was completed on September 30, 2016. Request Closure.

**Recommendation 17:** We recommended the Acting Assistant Secretary for Information and Technology consolidate the security responsibilities for networks, not managed by OI&T, under a common control for each site and ensure vulnerabilities are remediated in a timely manner. (This is a repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. VA MDPP and VHA have implemented a process to address device vulnerabilities on local facility systems not managed by OI&T. Additionally, VA's Medical Device Protection Program (MDPP) and VHA have implemented a process to address device vulnerabilities on local facility systems not managed by OI&T. Medical device cybersecurity is a shared responsibility between the device manufacturer and VA, each having separate stakeholder objectives. VA is to balance patient safety, regulatory requirements from the Food and Drug Administration, and overall access for patient care with cybersecurity. These standards and regulations include the following:

- Networked medical devices are federally regulated by the FDA 510K process, and configuration changes to improve the security of the devices/systems (e.g., software patching) is to be approved by the medical device manufacturer prior to implementation. The FDA, through its regulatory statutes, holds the medical device manufacturer responsible for the safety and efficacy of the device throughout its life cycle. Alterations to the configuration of the device without manufacturer's written approval will transfer the risk of failure in the safe and effective use of that device from the manufacturer to the healthcare delivery organization.
- VHA Biomedical Engineering is to obtain written approval from the medical device manufacturer prior to upgrading, updating, patching, or modifying medical device software. Medical device software includes, but is not limited to: medical device specific application software, commercial off the shelf (COTS) operating systems, COTS application software, and COTS malware protection software [NFR IT-2016-10 Vulnerability Configuration Management].

Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to December 31, 2016 include:

- VA OI&T has accepted responsibility for devices connected to VA's network through the issuance of policy that requires networked connected devices, tenant networks and medical devices to be accounted for as part of the existing GSS, making the system owner responsible for the devices connected to VA's network in their system boundary area or responsibility
- Devices connected to VA's network were documented and inventoried in March 2016 in a SSP addendum that identified the business owner, administrator and cyber security status of the equipment. These documents were added to the GRC tools as security artifacts.
- As of the end of FY16, the Medical Device Vulnerability Management Program achieved 92% compliance for the remediation of identified vulnerabilities. The remaining 8% of the medical device vulnerabilities had POA&Ms created for tracking and remediation in the GRC tool.
- POA&Ms have been opened for the medical devices that are running an unsupported operating system and where the vendor of the medical device has not accepted installing/implementing remediation steps and is being tracked within the GRC tool.
- OIS has developed a Medical Device Security Control Overlay (MDSCO) that identifies security control specifications needed to safeguard medical devices and the information stored, processed, or transmitted by these devices. This overlay provides a control set that will be used to standardized system security requirements and/or compliance across multiple medical device types and their associated systems.
- VA's SPS vulnerability program addresses identified vulnerabilities with local non-IT managed devices that provide mission essential services to the facility. Additional accomplishments include:
- An SPS process for vulnerability remediation has been created and implemented into the field. To support this, the OIS team has:
    - Created a process for remediation of SPS devices
    - Identified system owners within OI&T and VHA branches of VA
    - Identified which devices OI&T owns as well as outdated devices which will need to be upgraded in the future
    - Created a SOP and lessons learned to remediate vulnerabilities going forward
    - Conducted trainings for ISOs and facility members on how to remediate vulnerabilities going forward
    - Completed implementation of vulnerability remediation throughout the Enterprise

POA&Ms have been opened for the SPS that are running an unsupported operating system and where the vendor of the SPS has not accepted installing/implementing remediation steps and is being tracked within the GRC tool. Implementing this process has significantly improved network access controls and appropriately segregate mission-critical special purpose systems from the general network [QC Validation FISMA 15-01957-100 Recommendation 19].

As part of the overall project requirements, task validation was performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project was completed on December 31, 2016. Request Closure.

**Recommendation 18:** We recommended the Acting Assistant Secretary for Information and Technology implement improved processes to ensure that all devices and platforms are evaluated using credentialed vulnerability assessments. (This is a new recommendation.)

**OI&T Response:** VA concurs with this recommendation. VA is currently conducting the final testing phase of a project to enable authenticated scans across major Operating Systems on the network. Efforts are also underway to expand credentialed scans to other devices including MAC, UNIX/Linux, other network devices (including Cisco), printers, and IP phones. The processes for credentialed scanning of these devices have been established and the NSOC is currently performing a gap analysis and working with system owners to remediate issues that are preventing effective credentialed scans [NFR IT-2016-09 Vulnerability Configuration Management].

Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to April 27, 2017 include:

- Identified MAC, other Unix/Linux OS, network, and other devices across VA Enterprise
- Developed and tested MAC, other Unix/Linux OS, network, and other devices scan policies
- Completed regional credentialed MAC, other Unix/Linux OS, network, and other devices scan process testing
- Received approval for credential distribution method from National Change Control Board

Remaining ECST project activities are scheduled to be completed by June 30, 2017 and include the following tasks:

- Release National Action Item for distribution of new credentials
- Implement credentialed MAC, other Unix/Linux OS, network, and other devices scan processes
- Perform gap analysis of devices not providing credentialed scans
- Collaborate with System Owners to remediate scanning issues to receive effective credentialed scans.

As part of the overall project requirements, task validation will be performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project is targeted for completion by June 30, 2017.

**Recommendation 19:** We recommended the Acting Assistant Secretary for Information and Technology implement improved procedures to enforce a standardized system development and change control framework that integrates information security throughout the life cycle of each system. (This is a modified repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. In response to the repeat recommendation identified during the FY15 OIG FISMA audit, VA created a project to address the tactical security issues identified. Through the project, VA focused on providing training and accountability for individuals with change management responsibilities. VA has put effort into incorporating standardized system development and change management principles across the enterprise to instill a process whereby ad hoc and out-of-band system changes, even if intended to enhance customer experience, are not permitted. Specifically, VA OI&T staff are required to finish the Change Management training and record their results in VA TMS. Configuration management training was developed for standardized system development and change control management [QC Validation FISMA 15-01957-100 Recommendation 20].

Project efforts saw the incorporation of change management responsibilities into the newly formed Change Governance Working Group to escalate change management policy and ownership issues to the Information Security Governance Board. This aims to organize programmatic efforts as they relate to change management and security configuration management with the support of executive leadership [QC Validation FISMA 15-01957-100 Recommendation 20].

Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to December 31, 2016 include:

- Developed and signed charter to establish a working group to provide oversight and implementation of standard change and configuration management policies and procedures
- Conducted a gap analysis of the current VA change control process
- Developed configuration management training for standardized system development and change control management.

As part of the overall project requirements, task validation was performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project was completed on December 31, 2016. Request Closure.

**Recommendation 20:** We recommended the Acting Assistant Secretary for Information and Technology implement improved processes to ensure information system contingency plans are updated with the required information. (This is a modified repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. VA has implemented annual processes to confirm information system contingency plans are updated with the required information. Additional steps will be taken to confirm system owner's review and update their plans as required. The requirement to update and test system contingency plans is an annual event and is outlined in VA Handbook 6500.8, Information System Contingency Planning (ISCP). Each year, OIS provides guidance in the form of an action item that provides milestones, templates and actions that need to be completed. During the course of this action, training is provided to Division Chiefs as well as System Owners (or designee). Draft plans are reviewed by Regional Division Chiefs for operational feasibility and OIS Mentors provide feedback as to whether plans are compliant with VA and NIST guidance. After contingency plans are reviewed and accepted (pending required changes) by OIS, the system owner signs the plan and uploads to the GRC tool [NFR IT-2016-03 Contingency Planning].

The OIS Office of Business Continuity (OBC) created a maturity model that was applied enterprise-wide in a combined effort with ITOPS in FY16. The Risk Management Division completed a random validation of facility and systems ISCP using NIST 800-53A controls CP-1: Contingency Planning Policy and Procedures and CP-2: Contingency Plan. The review found that the 1% of ISCPs randomly sampled from a population of 720 were compliant with CP-1 and CP-2. A subsequent random review of an additional 1% of ISCPs found that the sample was compliant with using the new template and were dated 2016 [QC Validation FISMA 15-01957-100 Recommendation 21].

Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to December 31, 2016 include:

- Conducted a compliance review and assessment of IT contingency plans and captured their status from RiskVision and from the Information System Contingency Planning Assessment (ISCPA) tool
- Implemented the process for annual review of contingency plans to confirm information within is careful and up to date
- Implemented the process to annually test contingency plans to determine effectiveness

- Created a SOP to annually test contingency plans and failover capabilities for major applications and general support systems.

As part of the overall project requirements, task validation was performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project was completed on December 31, 2016. Request Closure.

**Recommendation 21:** We recommended the Acting Assistant Secretary for Information and Technology implement improved processes for ensuring the encryption of backup data prior to transferring the data offsite for storage. (This is a modified repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. In the first phase of a multi-phased process, VA purchased hardware and software to encrypt backup tapes for mission critical systems, including VistA. The installation of VistA system backup encryption was completed December 30, 2014. The encryption of VistA data was prioritized given the frequency of transport to off-site storage facilities and contains sensitive patient data. Planning for the next phase of encrypting mission critical systems (excluding Exchange, as OI&T is transitioning from Exchange to Office 365; encryption requirement will be addressed after transitioning to Office 365) is currently underway. In this phase, the backups of office automation data copied from disk-to-disk will be encrypted as appropriate and saved on network attached storage systems in secure locations. The plan to confirm encryption of backup data at rest is anticipated to be completed by the end of FY2017. In turn, unencrypted backup tapes shall not leave protected VA space, thus reducing the risk of lost / stolen tapes [NFR IT-2016-03 Contingency Planning].

Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to April 27, 2017 include:

- Began identifying and confirming that backup tapes are compliant with Federal Information Processing Standards (FIPS) 140-2 encryption
- Released a series of data calls to field offices as part of an ongoing effort to identify non-compliant sites and implement a FIPS 140-2 encryption solution

Remaining ECST project activities are scheduled to be completed by September 30, 2017 and include the following tasks:

- Procure a FIPS 140-2 standard backup tape encryption solution
- Implement and deploy a backup tape encryption solution.

As part of the overall project requirements, task validation will be performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project is targeted for completion by September 30, 2017.

**Recommendation 22:** We recommended the Acting Assistant Secretary for Information and Technology implement improved processes for the testing of contingency plans and failover capabilities for critical systems to ensure that all components can be recovered at an alternate site in the event of a system failure or disaster. (This is a modified repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. VA has implemented annual processes to confirm ISCPs are updated with the required information. Additional steps will be taken to confirm system owners are reviewing and updating their plans as required. Updates to VA information systems security contingency plans are influenced by several ongoing initiatives: the development of a systems inventory as part of the FY 2015 enterprise cybersecurity strategy, the identification of HVA in response to the Federal CIO's July 2015, Cyber Sprint Memorandum, current coordination with the Office of OSP to

correlate the HVA inventory with those information systems identified as part of their Business Impact Analysis (BIA) reassessment, and the FY 2015 MyVA Regional re-alignment which affected several system accreditation boundaries. The net result will aligned OI&T VA information systems contingency plans with its VA business partners [NFR IT-2016-03 Contingency Planning].

The requirement to update and test system contingency plans is an annual event and is outlined in VA Handbook 6500.8, Information System Contingency Planning. Each year, OIS provides guidance in the form of an action item that provides milestones, templates and actions that need to be completed. During the course of this action, training is provided to Division Chiefs as well as System Owners (or designee). Draft plans are reviewed by Regional Division Chiefs for operational feasibility and OIS Mentors provide feedback as to whether plans are compliant with VA and NIST guidance. After contingency plans are reviewed and accepted (pending required changes) by OIS, the system owner signs the plan and uploads to the GRC tool [NFR IT-2016-03 Contingency Planning].

For FY16, the ISCPA process achieved a complete update of the systems listed within the GRC tool. This includes approximately 720 ISCPs and Disaster Recovery Plans. This does not include plans submitted by EO for review and approval. Plans submitted by EO are handled throughout the year based on their year-around update process The results of this effort resulted in the "VA Material Weakness" tag being removed from contingency planning, one that has labeled contingency plans for the past 16 years. Fifteen of the sites audited had zero (0) findings associated with Contingency Planning. Of the nine sites listed by the IG as having findings, four of those had two or less. Three (3) sites audited by the IG accounted for 14 of the approximate 20 findings [NFR IT-2016-03 Contingency Planning].

Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to April 20, 2017 include:

- Assigned authority to conduct annual test of contingency plans and failover capabilities for major applications and general support systems
- Identified possible testing scenarios via tabletop exercises, checklists, parallel or full interrupt simulations, and scale of test based upon FIPS 199 impact level of the information system
- Created SOP to annually test contingency plans and failover capabilities for major applications and general support systems
- Developed process to annually test contingency plans and failover capabilities for major applications and general support systems
- Implemented process to annually test contingency plans and failover capabilities for major applications and general support systems based on the system / site categorization levels.

As part of the overall project requirements, task validation was performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project was completed on May 3, 2017.

**Recommendation 23:** We recommended the Acting Assistant Secretary for Information and Technology document a Business Impact Analysis for all systems and incorporate applicable Recovery Point Objectives for those systems. (This is a modified repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. VA concurs with this recommendation and will confirm that systems' BIA include Recovery Point Objectives (RPOs) for each system and those objectives are incorporated into an overall contingency planning strategy development effort. In addition, VA will update system BIAs on a periodic basis. Although VA concurs that this finding was valid, it should be noted that this condition was found only at the Austin ITC (AITC) and does not reflect on the VA

enterprise nor does it deserve a national finding. As noted on the AITC exit briefing, this condition was corrected at the time of the visit [NFR IT-2016-03 Contingency Planning].

VA Handbook 6500.8, ISCP managed by the OBC requires completion of the BIA as a component of the ISCP. EO has a BIA for its customers and incorporates the results into the ISCP process as table tops, or functional exercises are conducted [NFR IT-2016-03 Contingency Planning].The plan of action pertaining to this recommendation was closed based on the focus of the corrective action. However, OBC provides instructions for completion of ISCPs that includes how to collect BIA data from business owners and how to incorporate it into the ISCP strategy. OBC is currently working with EO to confirm their BIA is consistent with the collection process identified by OBC, including capturing RPO information [NFR IT-2016-03 Contingency Planning].

Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to June 30, 2017 include:

- Developed an SOP to annually perform and document BIAs within the Contingency Plan
- Implemented a process to annually perform and document BIAs for systems according to type of system/site categorization level.

As part of the overall project requirements, task validation was performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project was completed on June 30, 2016. Request Closure.

**Recommendation 24:** We recommended the Acting Assistant Secretary for Information and Technology identify all external network interconnections and implement improved processes for monitoring VA networks, systems, and connections for unauthorized activity. (This is a repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. VA will conduct an inventory of VA sites to identify external connections on an ongoing basis and as new connections are reported. Analysis of each identified connection will occur once reported and those that are found to be non-compliant will enter into a transition to be migrated to VA TIC Gateways and decommissioned thereafter. Non-compliant connections will be brought under the control of NSOC Security [NFR IT-2016-08 Security Incidents and Audit Logging].

Contractor hosting facilities connections are monitored by VA NSOC Compliance Scanning Services (CSS) Team that fulfills continuous monitoring requirements for VA systems hosted outside VA's network with the use of the internal Tenable Security Center Console method to communicate with remote scanners established inside business partner networks. This vulnerability scanning will be expanded to new remote Business Partner and their remote IP will be a function of the business partner's network and unknown to the CSS team until the remote scanner is configured. VA Directive and Handbook 6513, Secure External Connections, governing the process for managing and continuously monitoring VA connections is in final review [NFR IT-2016-08 Security Incidents and Audit Logging].

Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to April 27, 2017 include:

- Reviewed 1,500+ site responses noting external interconnections at the responding sites
- Confirmed mechanism in place at each site visited to continuously monitor external interconnections
- Deployed remediation teams to perform onsite assessments of external interconnections, where required

- Continued to remediate / mitigate risk for non-compliant connections

Remaining ECST project activities are scheduled to be completed by September 30, 2017 and include the following tasks:

- Identify external network connections
- Enforce Trusted Internet Connection 2.0 compliance
- Hold transition meetings with FCIO, system owner, business partner, and ISOs for newly identified noncompliant connections
- Implement telecommunication closet review of external connections
- Evaluate, assess, and test each newly identified connection's security posture.

As part of the overall project requirements, task validation will be performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project is targeted for completion by September 30, 2017.

**Recommendation 25:** We recommended the Acting Assistant Secretary for Information and Technology implement more effective agency-wide incident response procedures to ensure timely reporting, updating, and resolution of computer security incidents in accordance with VA standards. (This is a repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. VA NSOC initiated a Cyber Incident Response Working Group (IRWG) in March 2014, to improve VA's Incident Response capability. The work group consists of analysts and engineers across the NSOC. The goal of the IRWG is to review current cyber security incident response policies, procedures, and performance measures. The work group provided recommendations, which resulted in process updates, and an Executive Decision Memo dated March 24, 2014, mandating field personnel adhere to established VA NSOC remediation guidance. Additionally, the IRWG established a recurring conference call between VA NSOC, FSS, and ITOPS to facilitate situational awareness on open tickets and their remediation progress [NFR IT-2016-08 Security Incidents and Audit Logging].

VA NSOC also established monthly metrics to track the effectiveness of the incident response capability and reporting to the US Computer Emergency Readiness Team (US-CERT) via the Monthly Performance Review. In September 2015, the IRWG updated the VA NSOC Incident Response Plan (IRP) to include identified incidents are remediated in a timely manner and a FISMA requirement to track enterprise-wide metrics for incident response. Over FY15, time to containment of incident ticket was reduced from 22 days to one day on average. OIG noted that VA had implemented a set of metrics and monitoring procedures to assist with incident response. The new monitoring has allowed VA to affect a downward trend in ticket closure timespan [NFR IT-2016-08 Security Incidents and Audit Logging].

Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to April 27, 2017 include:

- Implemented new Security Incident Response policies and plans in an updated NSOC IRP
- Performed gap analysis between requirements and current state of agency-wide incident response procedures, resulting in an NSOC Incident Response Procedures document
- Established Cyber Incident Response Working Group to improve coordination between VA entities with incident response roles
- Reduced time to containment and time to closure of incident response tickets

Remaining ECST project activities are scheduled to be completed by September 30, 2017 and include the following tasks:

- Evaluate and improve VA ticketing system metrics
- Develop training and communications plans for timeliness resolution of computer security incidents in coordination with the Human Capital domain
- Review solution to confirm timely resolution of computer security incidents.

As part of the overall project requirements, task validation will be performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project is targeted for completion by September 30, 2017.

**Recommendation 26:** We recommended the Acting Assistant Secretary for Information and Technology ensures that VA's Network Security and Operations Center has full access of all security incident data to facilitate an agency-wide awareness of information security events. (This is a new recommendation.)

**OI&T Response:** VA concurs with this recommendation. VA NSOC has full access to reported cyber security incidents data in CA Service Desk or Remedy Privacy Security Event Tracking System (PSETS). Users have an obligation to report suspected cyber security incidents to their respective ISOs or the Enterprise Service Desk (ESD). In addition, the EO reports suspected cyber incidents or suspicious network traffic to VA NSOC via CA ticketing system. A copy of the ticket creation SOP is attached for review and consideration.

**Target Completion Date:** This project is complete. Request Closure.

**Recommendation 27:** We recommended the Acting Assistant Secretary for Information and Technology implement improved safeguards to identify and prevent unauthorized vulnerability scans and data exfiltrations from VA networks. (This is a modified repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. VA is researching several solutions to address the prevention of unauthorized scans. VA is in the process of baselining traffic from devices used at medium and large facility across VA. Once VA develops a network traffic baseline, VA will be able to create specialized triggers that will alert on correlation activity that is consistent with scanning activity. VA plans to develop this capability within the enterprise SIEM [NFR IT-2016-08 Security Incidents and Audit Logging].

In 2015, VA began implementing additional features to further protect VA against exfiltration of data. In addition, VA is continuing to explore longer term solutions to further protect veteran information. Email security appliances have improved the ability to identify Social Security Numbers within unencrypted email. This has improved the capabilities to include matching patterns that were not identified in earlier versions/technologies. Specific outbound protocols have been limited through the TIC. Port and application whitelisting exceptions are documented via RBD, which is an ongoing effort. A Secure Sockets Layer / Transport Layer Security (SSL/TLS) decryption and inspection capability pilot began in spring 2015 and is ongoing, and will be expanded and put into production using the Application Firewall Solution [NFR IT-2016-08 Security Incidents and Audit Logging].

Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to April 27, 2017 include:

- Removed legacy ports/protocols no longer in active use (Initial effort; tuning to follow)
- Procured next generation application firewall solution at TIC gateways

- Implemented data leak prevention feature for VA email that traverses the TIC gateways
- Implemented blocking of unauthorized VPN applications at TIC gateways
- Implemented Secure Shell (SSH) whitelisting at TIC gateways
- Implemented App ID whitelisting at TIC gateways (Initial effort; tuning to follow)

Remaining ECST project activities are scheduled to be completed by June 30, 2017 and include the following tasks:

- Implement new firewall policy to cover new technologies in coordination with OCS
- Review of ACL / ports / protocols to determine conformance to the new firewall policy
- Implement application protocol whitelisting at TIC gateways
- Implement next generation application firewall solution for SSL decryption, data filtering, sandboxing analysis at TIC gateways
- Analyze long-term security architecture solutions, including client-level data loss prevention, rogue connection prevention, and encryption.

As part of the overall project requirements, task validation will be performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project is targeted for completion by June 30, 2017.

**Recommendation 28:** We recommended the Acting Assistant Secretary for Information and Technology fully develop a comprehensive list of approved and unapproved software and implement continuous monitoring processes to prevent the use of unauthorized software on agency devices. (This is a repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. VA has remediated 97% of "prohibited" systems, representing more than 16,000 systems. VA monitors scan reporting and analyzes it daily. VA also facilitates synchronization between Technical Reference Model (TRM) updates and SCCM reporting. Local change orders and national AI are drafted and distributed monthly. Software not classified within TRM is considered "unmanaged". A team of analysts works through the backlog of the unmanaged software currently installed on the network. This team utilizes the available tools (e.g., Business DNA [BDNA], SCCM, TRM, Google, SMA Vulnerability reports) to prioritize and analyze these titles and submit to TRM for review and classification. This team has also been asked to survey VA's network of end-users to determine business need for each of these software technologies prior to submission to TRM. On a monthly basis, VA identifies unapproved software and blacklists it from the network. This process began in March 2015, with over 57,000 software applications residing on VA's network. VA is using the TRM for adjudication and listing of approved software [QC Validation FISMA 15-01957-100 Recommendation 28; CRISP RSS Update, April 14, 2017].

VA is teaming with the Department of Homeland Security (DHS) to implement continuous monitoring capabilities as part of the Continuous Diagnostics and Mitigation (CDM) Program. VA is implementing McAfee Application Control (MAC) to develop and implement a whitelist that will be enforced on VA systems. MAC is expected to have agents to allow application discovery on applicable systems [QC Validation FISMA 15-01957-100 Recommendation 28].

Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to December 31, 2016 include:

- Developed a process to update the TRM site

- Implemented BDNA normalization monitoring tool within VA's environment
- Developed a training and communications plan for monitoring, preventing installation, and removing of unauthorized software
- Developed an SOP for unapproved, prohibited, and unmanaged software remediation
- Developed monthly configuration management vulnerabilities remediation reports
- Entered enterprise software titles into the TRM portal on a monthly basis
- Updated the TRM portal on a monthly basis with enterprise software titles which were previously not entered into the TRM portal
- Developed remediation reports for newly identified unapproved, prohibited, and unmanaged software across the enterprise on a monthly basis
- Removed of identified unapproved, prohibited and unmanaged software across the enterprise on a monthly basis.

As part of the overall project requirements, task validation was performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project was completed on December 31, 2016. Request Closure.

**Recommendation 29:** We recommended the Acting Assistant Secretary for Information and Technology develop a comprehensive software inventory process to identify major and minor software applications used to support VA programs and operations. (This is a repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. In FY16, the Office of Architecture, Strategy and Design (ASD) developed an up-to-date inventory of software platforms and applications used across the organization. ASD deployed the BDNA User Console and Data Platform to provide a broad, enterprise-view inventory of hardware and software technologies deployed across VA's network. BDNA combines data from multiple systems within VA, which includes IBM BigFix (formerly IBM Endpoint Manager) and SCCM, to include data from VA TRM. BDNA currently tracks more than 900,000 deployed hardware devices and over 24 million software instances across VA's Network. Additionally, BDNA utilizes Technopedia, which allows VA to normalize installed software and monitor industry-published software end-of-support (EOS) and end-of-life (EOL) data; thus, enabling the organization to make better informed technology decisions [QC Validation FISMA 15-01957-100 Recommendation 29].

As part of the project, VA performed procedure requirements gathering and gap analysis on VA's software inventory process, documented each technology listed on the Standards and Technology list and generated a Master Software Inventory. VA also conducted a gap analysis of software reflected in VA One-VA TRM to assess which software is no longer supported by vendors and developed a documentation and communication plan that addresses the new software inventory process [QC Validation FISMA 15-01957-100 Recommendation 29].I in addition to the inventory the ASD office maintains, the TRM provides a whitelist of software technologies and standards authorized for use to develop, operate, host, and maintain VA applications.

The TRM database also contains a blacklist of prohibited technologies. Entries on this list have undergone a strategic assessment based upon the nature of the technology. The TRM database contains guidance, along with known applicable constraints, on the permissible range of technologies or standards that a VA user, OI&T administration support team, or Project Development Team may select or use. The TRM is not intended to direct procurements, although each entry contains available VA licensing information, if known. Requests for an assessment of a technology or standard can be submitted through the TRM tool and will be assessed by subject matter specialists of the TRM Management Group. Technologies should be operated and maintained in accordance with Federal and Department security

and privacy policies and guidelines. Technologies or technical standards that are not listed on the Technology / Standard List are considered unapproved for use. Technologies and technical standards that do not appear on the TRM have not been assessed; either an assessment or a waiver signed by the Deputy CIO of ASD based upon a recommendation from the Architecture and Engineering Review Board, should be obtained in order to use the technology [QC Validation FISMA 15-01957-100 Recommendation 29].

VA looks forward to continuing its implementation of the DHS Continuous Diagnostics and Mitigation (CDM) program. CDM is intended to strengthen VA's capabilities in configuration management to identify cybersecurity risks on an ongoing basis and facilitate further service automation to improve our overall security posture [QC Validation FISMA 15-01957-100 Recommendation 29]. Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to December 31, 2016 include:

- Performed procedure requirements gathering and gap analysis on VA's software inventory process
- Documented technologies listed on the Standards and Technology list and generated a Master Software Inventory
- Conducted a gap analysis of software reflected in VA One-VA Technical Reference Model to assess which software is no longer supported by vendors
- Developed a documentation and communication plan that addresses the new software inventory process.

As part of the overall project requirements, task validation was performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project was completed on December 31, 2016. Request Closure.

**Recommendation 30:** We recommended the Acting Assistant Secretary for Information and Technology implement procedures for overseeing contractor-managed cloud-based systems and ensure information security controls adequately protect VA sensitive systems and data. (This is a repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. In response to the recommendation, VA created a project to address the tactical security issue identified. Accomplishments for this recommendation as reported via weekly ECST reporting from March 14, 2016 to September 30, 2016 include:

- Performed requirements gathering and gap analysis for contractor cloud based systems
- Drafted Cloud security policy that will enable the development of SOPs and field processes
- Revised standard contract templates to support contractor-managed cloud-based system policy.

As part of the overall project requirements, task validation was performed by VA's Q&C Team to confirm closure [QC Validation FISMA 15-01957-100 Recommendation 30].

**Target Completion Date:** This project was completed on September 30, 2016. Request Closure.

**Recommendation 31:** We recommended the Acting Assistant Secretary for Information and Technology implement mechanisms for updating systems inventory, including contractor-managed systems and interfaces, and provide this information in accordance with Federal reporting requirements. (This is a modified repeat recommendation from prior years.)

**OI&T Response:** VA concurs with this recommendation. VA has implemented mechanisms for updating the FISMA systems inventory, which includes contractor-managed systems and types of interfaces and interconnection agreements. Accomplishments for this recommendation as reported via weekly ECST reporting from March 14, 2016 to September 30, 2016 include:

- Updated mechanisms for maintaining FISMA inventory, which includes an annual review of their systems inventory for accuracy
- Engaged Contracting Office to determine contractor-managed systems
- Developed list of contractor-managed systems and interfaces.

As part of the overall project requirements, task validation was performed by VA's Q&C Team to confirm closure [QC Validation FISMA 15-01957-100 Recommendation 31].

**Target Completion Date:** This project was completed on September 30, 2016. Request Closure.

**Recommendation FY 2006-04:** We recommended the Assistant Secretary for Information and Technology ensure appropriate levels of background investigations be completed for all personnel in a timely manner, implement processes to monitor and ensure timely reinvestigations on all applicable employees and contractors, and monitor the status of the requested investigations.

**OI&T Response:** VA concurs with this recommendation. Within OSP, the Personnel Security & Suitability (PSS) PMO is in the process of procuring and implementing a VA-wide VA Central Adjudication and Background Investigation System (VA-CABS), integrated with ICAM Onboarding solution, which will establish business rules based on the position description and the sensitivity to conduct investigations and re-investigations. VA-CABS will also monitor investigations and at the 4.5 year mark, a system generated message will be sent to security personnel to initiate the re-investigation process. This will decrease the number of individuals with outdated investigations [NFR IT-2016-02 – Background Investigations].

OSP has formed the ICAM PMO at the direction of the Deputy Secretary of VA. The ICAM mission is to establish an enterprise-wide standardized, integrated, and automated process for onboarding, monitoring, and off-boarding VA employees, contractors, trainees, and affiliates via an automated solution (hereby referred to as the ICAM Onboarding solution). Two critical components of the ICAM Onboarding solution will be the integration with HR-Smart (an authoritative Human Resource Information System [HRIS] deployed by VA as a replacement to PAID), and integration of USA Staffing (which notifies both HR-Smart and the ICAM Onboarding Solution and when an Employee has accepted an offer). The ICAM Onboarding Solution will serve as the authoritative source for Contractor identity data. These authoritative sources will allow the ICAM Onboarding solution to establish different digital identities for Employees and Contractors, allowing for a shift from manual to automated processes used to initiate, track, re-initiate background investigations, drive and streamline account creation, and decrease account duplication within VA for Employees and Contractors [NFR IT-2016-02 – Background Investigations].

In addition to USA Staffing and HR-Smart, the ICAM Onboarding Solution connects to downstream VA systems such as, AD, TMS, Veterans Affairs Personnel Accountability System (VA-PAS), and Electronic Contract Management System (ECMS). Future versions of the system will provide a portal by which VA volunteers and affiliates information can be entered directly into the centralized ICAM Onboarding solution [NFR IT-2016-02 – Background Investigations]. Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to April 27, 2017 include:

- Developed COR personnel security training requirements and curriculum
- Developed training and communications processes and requirements
- Developed FTE Requirement for oversight/compliance efforts to enforce investigations

- Updated VA Handbook 0710, Personnel Security and Sustainability Program
- Deployed fingerprint capture system equipment
- Created SOP and checklist and provided trainings for local facilities to track and initiate reinvestigations for employees in high risk positions in a timely manner.

Remaining ECST project activities are scheduled to be completed by December 31, 2017 and include the following tasks:

- Develop program for oversight inspections and program reviews (to include performance measures and reporting processes); Create a guide for assistance reading reports and remediating issues (ongoing)
- Implement improved processes to determine local facilities track and initiate reinvestigations for employees in high risk positions in a timely manner
- Select an enterprise-wide commercial off-the-shelf (COTS) case management system
- Conduct periodic oversight compliance evaluations of facility personnel security offices (PSS); execute oversight / compliance inspection checklists (ongoing).

As part of the overall project requirements, task validation will be performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project is targeted for completion by December 31, 2017.

**Recommendation FY 2006-09:** We recommended the Assistant Secretary for Information and Technology identify and deploy solutions to encrypt sensitive data and resolve clear text protocol vulnerabilities.

**OI&T Response:** VA concurs with this recommendation. As a result of this recommendation, VA created a project to complete the implementation of Group Encrypted Transport Virtual Private Network (GETVPN) on wide area network (WAN) data circuits to encrypt sensitive data in transit and to resolve clear text vulnerabilities. Accomplishments for this recommendation as reported via weekly ECST reporting from December 15, 2015 to March 31, 2017 include:

- VA identified devices required to encrypt sensitive data on VA networks.
- Through VA Group Encrypted Transport Virtual Private Network (GETVPN) initiative, VA implemented GETVPN encryption on capable devices and installed new routers on WAN circuits, which were previously not capable of encrypting network flow traffic for Regions 1-6, VA HQ and EO.
- VA implemented Splunk to monitor WAN circuits for GETVPN compliance to identify and correct discrepancies.

As part of the overall project requirements, task validation was performed by VA's Q&C Team to confirm closure.

**Target Completion Date:** This project was completed on March 31, 2017. Request Closure.

# Appendix E Office of Inspector General Contact and Staff Acknowledgements

| | |
|---|---|
| Contact | For more information about this report, please contact the Office of Inspector General at (202) 461-4720. |
| Acknowledgments | Michael Bowman, Director<br>Carol Buzolich<br>Jerry Charles<br>Richard Purifoy<br>Juan Rivera<br>Felita Traynham |

# Appendix F Report Distribution

## VA Distribution

Office of the Secretary
Veterans Health Administration
Veterans Benefits Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel
Office of Acquisition, Logistics, and Construction
Board of Veterans Appeals

## Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs and Related Agencies
House Committee on Oversight and Government Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
Government Accountability Office
Office of Management and Budget
Department of Homeland Security

**This report is available on our website at www.va.gov/oig.**