DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

DEPARTMENT OF VETERANS AFFAIRS

Federal Information Security Modernization Act

Fiscal Year 2017

AUDIT | **REPORT #17-01257-136** | **April 11, 2018**

OIG MISSION

To serve veterans and the public by conducting effective oversight of the programs and operations of the Department of Veterans Affairs (VA)

In addition to general privacy laws that govern release of medical information, disclosure of certain veteran health or other private information may be prohibited by various federal statutes including, but not limited to, 38 U.S.C. §§ 5701, 5705, and 7332, absent an exemption or other specified circumstances. As mandated by law, the OIG adheres to privacy and confidentiality laws and regulations protecting veteran health or other private information in this report.

Report suspected wrongdoing in VA programs and operations to the VA OIG Hotline:

www.va.gov/oig/hotline

1-800-488-8244

Department of Veterans Affairs Memorandum

From: Assistant Inspector General for Audits and Evaluations

Subj: VA's Federal Information Security Modernization Act Audit for Fiscal Year 2017

To: Executive in Charge for Information and Technology

1. Enclosed is the final audit report, *Federal Information Security Modernization Act Audit for Fiscal Year 2017*. The Office of Inspector General contracted with the independent public accounting firm, CliftonLarsonAllen LLP, to assess the Department of Veterans Affairs' 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 programs 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. CliftonLarsonAllen LLP is responsible for the findings and recommendations included in this report. The OIG reviewed this report and related documentation for compliance with professional standards and contract requirements. The OIG review was not intended to express an opinion regarding the effectiveness of VA's information security program in place during FY 2017. Independent OIG auditors will follow up on the outstanding recommendations and evaluate the adequacy of corrective actions during their FY 2018 FISMA audit.

4. 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 2017 audit of VA's Consolidated Financial Statements;
    - 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; and

- 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;

5. This report provides 29 recommendations for improving VA's information security program: 27 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 information security control deficiencies were repeated during the FY 2017 FISMA audit. VA successfully closed four recommendations in FY 2017.

6. The effect of the open recommendations will be considered in the FY 2018 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

Abbreviations

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
VA	Department of Veterans Affairs

CliftonLarsonAllen LLP
www.claconnect.com

March 19, 2018

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 Modernization Act of 2014 (FISMA) for the federal fiscal year ending September 30, 2017 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. The audit was performed in accordance with *Generally Accepted Government Auditing Standards*, issued by the Comptroller General of the United States. 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 2017 through November 2017. 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 October 2017. 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 E, and is not intended to be and should not be used by anyone other than these specified parties.

Sincerely,

CliftonLarsonAllen LLP
Arlington, Virginia

TABLE OF CONTENTS

I. OBJECTIVE 1

II. OVERVIEW 1

III. RESULTS AND RECOMMENDATIONS **2**

1. Agency-Wide Security Management Program 2

A. Progress Made While Challenges Remain 2

B. Risk Management Strategy 3

C. Plans of Action and Milestones 3

D. System Security Plans 4

2. Identity Management and Access Controls 5

A. Password Management 5

B. Access Management 5

C. Audit Logging and Monitoring 6

D. Strong Authentication 6

3. Configuration Management Controls 7

A. Unsecure Web Applications and Services 7

B. Unsecure Database Applications 7

C. Application and System Software Vulnerabilities 7

D. Unsecure Network Access Controls 8

E. Baseline Security Configurations 8

4. System Development and Change Management Controls 9

5. Contingency Planning 10

6. Incident Response and Monitoring 11

A. Some Interconnections Not Monitored 11

B. Network Monitoring Needs Improvement 11

7. Continuous Monitoring 12

A. Inconsistent Security Control Assessments 13

B. Software Inventory Processes Need Improvement 13

8. Contractor Systems Oversight 14

APPENDIX A: STATUS OF PRIOR YEAR RECOMMENDATIONS 16

APPENDIX B: BACKGROUND 17

APPENDIX C: SCOPE AND METHODOLOGY 19

APPENDIX D: Executive in Charge FOR INFORMATION AND TECHNOLOGY COMMENTS 21

APPENDIX E: REPORT DISTRIBUTION 53

I. 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 2017 FISMA audit.

II. 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 44 major applications and general support systems at 24 VA facilities. In FY 2017, 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 29 total recommendations for improving VA's information security program. Twenty-seven 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 four recommendations in FY 2017. The FY 2016 FISMA report provided 33 recommendations for improvement.

III. RESULTS AND RECOMMENDATIONS

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.

A. Progress Made While Challenges Remain

In FY 2017, the VA's Chief Information Officer continued the Enterprise Cybersecurity Strategy Team (ECST) initiative including the 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
- Expanded enforcement of two-factor authentication to access network resources
- Continued maturation of an IT governance, risk, and compliance tool to improve processes for assessing, authorizing, and monitoring the security posture of VA systems
- Further enhancements and use of the centralized audit log collection and analysis tool

However, the aforementioned 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 mature the process related to its 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 to include risk management processes, plans of actions and milestones, and system security documentation. 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.

B. 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 always consider all known system security risks and threat sources. Specifically, we identified system Risk Assessments that did not address potential external attacks, human error, previously identified security weaknesses, or significant threat sources such as risks associated with systems not managed by the Office of Information and Technology (OI&T). We also identified issues related to the inaccurate reporting of the status for certain system security controls and noted that two systems were granted Authority to Operate without undergoing an assessment of security controls.

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 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.

C. 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 8,500 open POA&Ms in FY 2017 as compared with 7,200 open POA&Ms in FY 2016. VA has 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 milestone dates, (b) POA&M items that were not updated within the GRC tool to accurately reflect their current status, and (c) POA&Ms were not consistently updated to consider all known security weaknesses.

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.

D. System Security Plans

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 VA inaccurately reported the status of certain security controls within their regional level system security plans. Additionally, while medical devices and special purpose systems were appropriately included within the regional network boundaries, the implementation of specific controls for these devices were not addressed within regional level system security plans.

CORRECTIVE ACTIONS RECOMMENDED

1. We recommended the Executive in Charge 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.)*

2. We recommended the Executive in Charge 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.)*

3. We recommended the Executive in Charge for Information and Technology implement improved processes to ensure that all identified weaknesses 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.)*

4. We recommended the Executive in Charge 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.)*

5. We recommended the Executive in Charge for Information and Technology develop mechanisms to ensure system security plans reflect current operational environments, include an accurate status of the implementation of system security controls, and all applicable security controls are properly evaluated. *(This is a modified repeat recommendation from prior years.)*

6. We recommended the Executive in Charge for Information and Technology implement improved processes for reviewing and updating key security documents such as risk assessments and security control assessments on an annual basis and ensure the information accurately reflects the current environment. *(This is a modified repeat recommendation from prior years.)*

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

A. 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.

B. Access Management

VA has increased the overall enforcement of strong authentication for its systems and networks. 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.

C. Audit Logging and Monitoring

While VA continues to improve its centralized Security Incident and Event Management processes, we continue to identify deficiencies with how audit logs and security events are managed throughout the enterprise. For example, VA did not consistently review security violations and audit logs supporting mission-critical systems. Specifically, we noted that security logs were not effectively managed, aggregated, or proactively reviewed for certain significant systems, such as Veterans Health Information Systems and Technology Architecture, and users with elevated privileges. VA Handbook 6500, Appendix F provides high-level policy and procedures for collection and review of system audit logs. Audit log collections and 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.

D. Strong Authentication

VA has made progress in implementing strong authentication for remote and local network access. However, we noted that two-factor authentication for local network access was not fully implemented across the agency for much of FY 2017. 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.

CORRECTIVE ACTIONS RECOMMENDED

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

8. We recommended the Executive in Charge 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.)*

9. We recommended the Executive in Charge for Information and Technology enable system audit logs on all critical systems and platforms and conduct centralized reviews of security violations across the enterprise. *(This is a repeat recommendation from prior years.)*

10. *We recommended the* Executive in Charge for Information and Technology fully implement two-factor authentication for all network access methods throughout the agency. *(This is a repeat recommendation from prior years.)*

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, accurate system and software inventories, 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, vulnerable third-party applications and operating system software, and a lack of common platform security standards and monitoring across the enterprise.

A. Unsecure Web Applications and Services

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 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.

Additionally, we noted that VA was unable to provide an accurate inventory of devices running web applications at local facilities. While VA uses a process to identify web based vulnerabilities, such as Structured Query Language injection attacks on major systems, this process was not applied to all web based systems across the enterprise. Consequently, we continue to identify significant security vulnerabilities on web applications hosted at local facilities.

B. 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.

C. 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.

We also 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. Furthermore, 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 more effectively remediate vulnerabilities identified in operating systems, databases, applications, and other network devices.

D. 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 VA's general network.

VA did not perform comprehensive and credentialed vulnerability 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) certain configuration and management consoles for device networking, (2) audio testing device images, and (3) audiology test results to include sensitive patient information. We also identified public kiosks which allowed unauthorized file system access.

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.

E. 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 or monitored on all VA platforms. 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. In addition, VA has not fully documented or approved security baseline standards for all of its

systems. VA is working towards 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.

CORRECTIVE ACTIONS RECOMMENDED

11. We recommended the Executive in Charge 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.)*

12. We recommended the Executive in Charge 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.)*

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

14. We recommended the Executive in Charge 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.)*

15. We recommended the Executive in Charge 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.)*

16. We recommended the Executive in Charge for Information and Technology implement improved processes to ensure that all devices and platforms are evaluated using credentialed vulnerability assessments. *(This is a repeat recommendation from prior years.)*

4. SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT CONTROLS

VA has not consistently followed 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 two major data centers and five VA medical centers, 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.

CORRECTIVE ACTIONS RECOMMENDED

17. We recommended the Executive in Charge 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 repeat recommendation from prior years.)*

5. CONTINGENCY PLANNING

VA contingency plans were not consistently and comprehensively tested to ensure failover capability to alternate processing sites and to ensure recovery efforts could be accomplished at designated locations. Additionally, VA data was not always adequately protected in accordance with established policy. 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.

- Backup tapes for certain mission-critical systems were not encrypted prior to transporting data offsite for storage. We identified this issue at two major data centers and twelve VA medical centers.
- Contingency plans were not comprehensively tested to ensure failover capability to alternate processing sites. Specifically, we identified this issue at eleven VA medical centers and the Capital Region Readiness Center. We also noted that certain financial applications could not be recovered within stated Recovery Time Objectives during annual contingency and disaster recovery exercises.

CORRECTIVE ACTIONS RECOMMENDED

18. We recommended the Executive in Charge 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 repeat recommendation from prior years.)*

19. We recommended the Executive in Charge 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 the assigned sites and within stated timeframes. *(This is a modified repeat recommendation from prior years.)*

6. INCIDENT RESPONSE AND MONITORING

VA made progress in relation to its overall incident response program, network protection, and monitoring capabilities. Additional procedures, such as the collection and monitoring of additional incident response metrics have allowed VA to strengthen its incident response and network security program. However, deficiencies were noted in several areas including security event monitoring, security event correlation, network sensor coverage, vulnerability scan monitoring, and data exfiltration safeguards.

A. Some Interconnections Not Monitored

VA does not monitor all external interconnections and internal network segments for malicious traffic or unauthorized systems access attempts. Specifically, we noted that VA has 12 business partner external connections that are not currently monitored by one of its Trusted Internet Connection gateways. VA is working towards migrating unmonitored network connections into the Trusted Internet Connection gateways and currently has all connections identified within the national change approval process required for the migration. These business partner connections provide external entities with access to VA's network but they are not configured with the same security measures as monitored interconnections.

We noted that VA's Network and Security Operations Center was unable to perform adequate security testing of all systems across the enterprise. Consequently, VA did not have a complete inventory of all vulnerabilities present on locally hosted systems. Ineffective monitoring of internal network segments could prevent VA from detecting and responding to intrusion attempts in a timely manner. As a result, our audit continued to identify numerous high-risk security incidents, including malware infections that were not responded to in a timely manner. Specifically, we noted these issues at four major data centers, eleven VA medical centers, three Regional Offices, and the Insurance Center. 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 year.

During the year, VA continued monitoring additional performance measurements to assist with responding to security incidents. The new procedures allowed VA to improve security event response times as the year progressed. VA has implemented several tools including "Splunk" and "qRadar" to facilitate enhanced audit log collection and analysis. However, we noted the tools did not collect data from all critical systems and major applications. Additionally, VA's Network Security and Operations Center did not have full visibility to evaluate all security-related audit data throughout the enterprise for the entire year. Management plans to fully implement the "Splunk" tool across all platforms in support of an agency-wide Security Incident and Event Management solution.

B. 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.

CORRECTIVE ACTIONS RECOMMENDED

20. We recommended the Executive in Charge 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.)*

21. We recommended the Executive in Charge 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*.)

22. We recommended the Executive in Charge for Information and Technology ensure that VA's Network Security and Operations Center has full access to all security incident data to facilitate an agency-wide awareness of information security events. *(This is a repeat recommendation from prior years.)*

23. We recommended the Executive in Charge for Information and Technology implement improved safeguards to identify and prevent unauthorized vulnerability scans and data exfiltrations from VA networks. (*This is a repeat recommendation from prior years.*)

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 fully implemented for identifying and removing unauthorized application software on VA systems. 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.

A. 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 Office of Quality, Privacy, and Risk. This organization completed numerous security control assessments throughout the year utilizing a standardized methodology and approach. However, we identified issues with how the results of these assessments were evaluated in connection with continuous monitoring activities. Specifically, at nine VA medical centers, we noted that certain system security deficiencies were not incorporated into POA&M management and risk management activities in a timely manner.

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. 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.

B. Software Inventory Processes Need Improvement

At the time of our audit, VA had improved systems and data security control protections by enhancing the implementation of certain technological solutions, such as a 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 prohibited software, hardware devices, and system configurations.

CORRECTIVE ACTIONS RECOMMENDED

24. We recommended the Executive in Charge 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.)*

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

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 2017. 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 risk 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.

CORRECTIVE ACTIONS RECOMMENDED

26. We recommended the Executive in Charge for Information and Technology implement improved 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.)*
27. We recommended the Executive in Charge 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 repeat recommendation from prior years.)*

SUMMARY OF RESPONSE FROM THE EXECUTIVE IN CHARGE FOR THE OFFICE OF INFORMATION AND TECHNOLOGY

The Executive in Charge for the Office of Information and Technology generally 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 Executive in Charge stated that VA has closed all but one Plan of Actions during calender year 2017. The Executive in Charge also stated that VA is currently developing various projects to correct the items found in the FY 2017 audit using the now, near, and future timeframes. We will continue to evaluate VA's progress during our audit of VA's information security program in FY 2018. We remain concerned that continuing delays in implementing effective corrective actions by estimated completion dates to address these open recommendations can potentially contribute to reporting an information technology material weakness from this year's 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 Executive in Charge 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	To be determined	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. Exceptions related to timely background investigations continued to be identified during FY 2017 FISMA testing.
FY 2006–09	We recommended the Executive in Charge for Information and Technology identify and deploy solutions to encrypt sensitive data and resolve clear text protocol vulnerabilities.	In Progress	To be determined	VA has launched a project to encrypt sensitive data transmitted over external and internal data circuits and resolve clear text protocol vulnerabilities. Management states that this project was completed during FY 2017.

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 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 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 established current information security priorities and provided 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 provided 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 2017 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 2017. 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 44 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 2017 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.

1. 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—Albuquerque, NM
- VA Medical Facility—Ann Arbor, MI
- VA Medical Facility—Atlanta, GA
- Information Technology Center—Austin, TX
- Verizon, Cloud Service Provider—Culpepper, VA
- VA Medical Facility—East Orange, NJ
- Information Technology Center—Hines, IL
- VA Medical Facility—Houston, TX
- VA Regional Office—Houston, TX
- VA Medical Facility—Huntington, WV
- VA Regional Office—Huntington, WV
- Network Security Operations Center—Martinsburg, WV
- Capital Region Readiness Center—Martinsburg, WV
- VA Medical Facility—North Chicago, WV

- Information Technology Center—Philadelphia, PA
- VA Insurance Center—Philadelphia, PA
- VA Medical Facility— Phoenix, AZ
- VA Regional Office—Phoenix, AZ
- Loan Guaranty Contractor Managed Facility—Plano, TX
- VA Medical Facility—Providence, RI
- National Cemetery Administration—Quantico, VA
- VA Medical Facility—San Diego, CA
- VA Medical Facility—St. Louis, MO
- VA Central Office—Washington, DC

During site visits, we evaluated 44 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.

2. 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: EXECUTIVE IN CHARGE FOR INFORMATION AND TECHNOLOGY COMMENTS

Department of Veterans Affairs

Memorandum

Date: March 12, 2018

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

Subj: Draft OIG Report: Federal Information Security Management Act (FISMA) Assessment for FY 2017

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 2017.* All but one POA was closed during calendar year 2017. VA is currently developing various projects to correct the items found in the FY17 audit using the now, near, and future timeframes.

2. 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) 461-5139.

/s/ Scott R. Blackburn

Attachment

Attachment

Office of Information and Technology
Comments to Draft OIG Report,
"Federal Information Security Modernization Act Audit for FY 2017"
OIG Recommendations and OIT Responses:

Recommendation 1: We recommended the Executive in Charge 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 and continues to implement a risk assessment process to evaluate and manage the identified risks affecting information systems, as well as cybersecurity risks across the agency. The risk assessment process is being implemented as part of the ECSP refresh, initiated in 2017, which consists of the following:

- An update to the 2015 Enterprise Cybersecurity Strategy (ECS)
- Revisions to VA's core cybersecurity and risk management policies
- The establishment of a centralized policy and implementation guidance repository known as the Knowledge Service (KS),
- VA's implementation of the CSF and the RMF

The ECSP applies an integrated approach to managing cybersecurity risk by aligning system-level perspectives on cybersecurity risk through the RMF with the CSF to provide an enterprise view of cybersecurity risks. By proactively adopting and implementing statutory requirements related to cybersecurity risk management, VA is prepared to evaluate the relevant risks and evolving threat landscape in alignment with OMB expectations. VA is positioned to create an agency-level risk profile (CSF) that incorporates system-level risk (e.g., impact and likelihood of threats) to drive risk management decisions (e.g., operational, strategic, and budgetary) and enhance VA's overall cybersecurity posture in collaboration with Federal entities (e.g., DHS). Through the implementation of CSF and RMF, VA is expected to be in a position to proactively identify and assess the relevant risks commonly found in the risk environment.

VA continues to improve its RMF implementation to provide updated, targeted, and platform-based security guidelines for VA information systems through the accreditation boundary realignment and GRC refresh initiatives through Fiscal Year (FY) 2018. These initiatives enable better visibility and increased identification of risk across the information system landscape. Additionally, they will improve uniformity and accountability so that VA leadership has better insight into information system risks affecting VA's ability to meet mission and business objectives. As required, the Office of Cybersecurity (OCS) will work with system owners to update the risk assessments to incorporate relevant risks of the current operating environment.

Accomplishments for this Recommendation:

• Began integration of RMF and CSF to improve the overall cybersecurity risk management approach and enable informed decisions on how to reduce overall risk to VA

• Developed a risk profile that prioritizes risks that are significant threats to the accomplishment of VA's mission and objectives, as determined by OI&T leadership

• Implemented requirements related to cybersecurity risk management that allow VA to evaluate the relevant risks and evolving threat landscape

Began evolving ECSP in order to utilize risk-based metrics to prioritize remediation efforts, allocate resources, and address risks to secure VA mission / business processes. **Target Completion Date**: In Progress

Recommendation 2: We recommended the Executive in Charge 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. Oversight through SCAs, Case Management, Cyber Security Risk Management team, and field level activities are expected to confirm that application of security requirements and its supporting documentation, including POA&Ms, have been updated within the GRC tool. VA issued training to system stakeholders involved in POA&M management and continues to review existing POA&M workflows inherent within the GRC tool.

As a result of the VA transformation, ESL Cyber Security Risk Management Team will assist ITOPS in VA in monitoring the weaknesses until actions have been taken for the control and evidence is provided to support closure. POA&Ms that are not compliant per policy and guidance set forth in the POA&M Management guide are re-opened for appropriate action.

VA continues to develop oversight and compliance mechanisms to capture supporting documentation from System Owners that justify closure of POA&Ms. These efforts are intended to enhance execution based on policy and SOPs, which have been developed, including the POA&M Management guide. VA will reevaluate roles and responsibilities assigned to system stakeholders in order to refine and institutionalize expectations on a standard approach to POA&M creation, updates, and closure. VA will apply a consistent approach to the closure of POA&Ms by deploying a site level role that supports the review and updates to system level documentation, including POA&Ms.

Accomplishments for this Recommendation:

- Began execution of the Case Manager oversight activities in January 2018 as outlined within the CMPP
- Developed new templates for PIA and CP templates in an effort to enhance VA's existing GRC tool POA&M update process.
- Conducted training on POA&Ms with system owners and data stewards on how to upload artifacts to the GRC tool
- Issued POA&M Management Guide and Authorization Requirements SOP on POA&M requirements, roles and responsibilities, escalation procedures, and update processes
- Initiated a program to further define policies and improve training to increase system owner accountability

- 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
- Incorporated POA&M requirements into the Oversight and Compliance process that will allow POA&Ms to be captured, reviewed, and reported on
- Enhanced accountability structure to manage POA&M processing through functionality within GRC workflows and procedural reviews

Developed a cross functional compliance process for uploading POA&Ms identified during assessments where Security Control Assessment (SCA) findings are received through OCS, then vetted through the ESL Cyber Security Risk Management team prior to upload by OCS. VA is permitted 15 days to enter a response in accordance with the POA&M Management Guide. **Target Completion Date:** In Progress

Recommendation 3: We recommended the Executive in Charge 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 and will continue to expand its POA&M oversight and compliance capabilities through its Case Management, Security Control Assessments (SCAs), and Enterprise Service Line (ESL) Cyber Risk Management team efforts that aim to direct, evaluate, and monitor processes and resources involved within the system accreditation lifecycle to confirm that POA&Ms reflect the current state of the identified security weaknesses.

As a result of the VA transformation, the ESL Cyber Security Risk Management Team will address the inconsistencies in the POA&Ms throughout the enterprise. The team has implemented the practice of providing daily POA&M reports to the individual entities where POA&Ms are approaching their estimated closure date or date which to provide an update to the milestone/response. These reports facilitate daily monitoring for progress which is sent to the appropriate management officials and stakeholders for their awareness and action. In addition, the Quarterly POA&M Review Action Item assists VA in monitoring the weaknesses until sufficient actions have been taken for the control and sufficient evidence is provided for closure. POA&Ms that are not compliant per policy and guidance set forth in the POA&M Management guide are re-opened for appropriate action.

To strengthen its POA&M process and track and prioritize remediation activities for information systems through the Case Management function, VA provides system oversight enabling system owners to manage and to adequately address security vulnerabilities effectively, ultimately resulting in their closure and the ability to achieve broader compliance. The Case Management team, which began oversight activities in January 2018, provides timelines, monitors completion of tasks by System Owners and escalates non-compliance activities to VA Leadership in accordance with the escalation triggers in the Case Manager Performance Procedure (CMPP). A standardized POA&M process will result in VA's POA&Ms being consistently managed and remedial information security actions taking place to mitigate risk to VA operations, assets, individuals, other organizations.

In addition, VA reevaluated roles and responsibilities assigned to system stakeholders in order to determine an approach aimed at facilitating consistent POA&M creation, updates, and closure. As part

of this reassignment of responsibility, OIS began to remove system level ISO responsibilities from Risk Vision and transferred responsibilities to the ITOPS CRM Team. This approach by dedicated a team of specialized security practioners will afford consistency and validity of updating and documenting the system level POA&Ms. Additionally, per the CMPP, the Case Management function has defined the roles and responsibilities for parties involved in the POA&M tracking process, intended to clarify the overall POA&M process. The compliance and oversight activities, managed by the Case Manager team, will continue to evolve based on VA's requirements. By deploying a capability that is dedicated to working with facilities and system owners, the Office of Information Security (OIS) will support system owners to review, update, and continuously monitor security documentation, including POA&Ms, in alignment with VA's policies and standards. This capability will enable consistent and timely updates, and sustained oversight of the security state of information systems on an ongoing basis.

During Fiscal Year 2017, OCS began importing findings and creating POA&Ms in the Governance Risk and Compliance (GRC) tool for SCAs conducted under the authority of OCS and will continue timely POA&M creation. VA's RMF refresh initiatives through end of Fiscal Year (FY) 2017 and into 2018, such as the GRC refresh will provide automation to support the development and tracking of POA&Ms for timely remediation. Additionally, the Knowledge Service (KS), which was launched in January of 2018 will allow VA employees to learn more about security control policy and implementation guidance, Plan of Action and Milestones management and associated requirements, and information security and privacy requirements.

Accomplishments for this Recommendation:

- Began execution of the Case Manager oversight activities in January 2018 outlined within the CMPP
- Launched KS to serves as a centralized, user-friendly site for employees and contractors to access VA security policy and implementation guidance in support of the ECSP
- Developed new templates for Privacy Impact Assessment (PIA) and Contingency Planning (CP) templates in an effort to enhance VA's existing GRC tool POA&M update process.
- Conducted training on POA&Ms with system owners and data stewards on how to upload artifacts to the GRC tool
- Issued POA&M Management Guide and Authorization Requirements Standard Operating Procedures (SOP) on POA&M requirements, roles and responsibilities, escalation procedures, and update processes
- Initiated a program to further define policies and improve training to increase system owner accountability
- 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
- Incorporated POA&M requirements into the Oversight and Compliance process that will allow POA&Ms to be captured, reviewed, and reported on
- Enhanced accountability structure to manage POA&M processing through functionality within GRC workflows and procedural reviews
- Developed a cross functional compliance process for uploading POA&Ms identified during assessments where Security Control Assessment (SCA) findings are received through OCS, then vetted through the ESL Cyber Security Risk Management team prior to upload by OIS. VA is permitted 15 days to enter a response in accordance with the POA&M Management Guide

As of January 2018, the Case Management function saw an 11% decrease in the amount of open POA&Ms within its GRC tool. To support this effort, the Case Management team has coordinated with stakeholders for systems that require compliance attention. **Target Completion Date:** In Progress

Recommendation 4: We recommended the Executive in Charge 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 and will continue to expand its POA&M oversight and compliance capabilities through its Case Management, Security Control Assessments (SCAs), and Enterprise Service Line (ESL) Cyber Risk Management team efforts that aim to direct, evaluate, and monitor processes and resources involved within the system accreditation lifecycle to confirm that POA&Ms reflect the current state of the identified security weaknesses.

As a result of the VA transformation, the ESL Cyber Security Risk Management Team will address the inconsistencies in the POA&Ms throughout the enterprise. The team has implemented the practice of providing daily POA&M reports to the individual entities where POA&Ms are approaching their estimated closure date or date which to provide an update to the milestone/response. These reports facilitate daily monitoring for progress which is sent to the appropriate management officials and stakeholders for their awareness and action. In addition, the Quarterly POA&M Review Action Item assists VA in monitoring the weaknesses until sufficient actions have been taken for the control and sufficient evidence is provided for closure. POA&Ms that are not compliant per policy and guidance set forth in the POA&M Management guide are re-opened for appropriate action.

To strengthen its POA&M process and track and prioritize remediation activities for information systems through the Case Management function, VA provides system oversight enabling system owners to manage and to adequately address security vulnerabilities effectively, ultimately resulting in their closure and the ability to achieve broader compliance. The Case Management team, which began oversight activities in January 2018, provides timelines, monitors completion of tasks by System Owners and escalates non-compliance activities to VA Leadership in accordance with the escalation triggers in the Case Manager Performance Procedure (CMPP). A standardized POA&M process will result in VA's POA&Ms being consistently managed and remedial information security actions taking place to mitigate risk to VA operations, assets, individuals, other organizations.

In addition, VA reevaluated roles and responsibilities assigned to system stakeholders in order to determine an approach aimed at facilitating consistent POA&M creation, updates, and closure. As part of this reassignment of responsibility, OIS began to remove system level ISO responsibilities from Risk Vision and transferred responsibilities to the ITOPS CRM Team. This approach by dedicated a team of specialized security practioners will afford consistency and validity of updating and documenting the system level POA&Ms. Additionally, per the CMPP, the Case Management function has defined the roles and responsibilities for parties involved in the POA&M tracking process, intended to clarify the overall POA&M process. The compliance and oversight activities, managed by the Case Manager team, will continue to evolve based on VA's requirements. By deploying a capability that is dedicated to working with facilities and system owners, the Office of Information Security (OIS) will support system owners to review, update, and continuously monitor security documentation, including POA&Ms, in alignment with VA's policies and standards. This capability will enable consistent and timely updates, and sustained oversight of the security state of information systems on an ongoing basis.

During Fiscal Year 2017, OCS began importing findings and creating POA&Ms in the Governance Risk and Compliance (GRC) tool for SCAs conducted under the authority of OCS and will continue timely POA&M creation. VA's RMF refresh initiatives through end of Fiscal Year (FY) 2017 and into 2018, such as the GRC refresh will provide automation to support the development and tracking of POA&Ms for timely remediation. Additionally, the Knowledge Service (KS), which was launched in January of 2018 will allow VA employees to learn more about security control policy and implementation guidance, Plan of Action and Milestones management and associated requirements, and information security and privacy requirements.

Accomplishments for this Recommendation:

- Began execution of the Case Manager oversight activities in January 2018 outlined within the CMPP
- Launched KS to serves as a centralized, user-friendly site for employees and contractors to access VA security policy and implementation guidance in support of the ECSP
- Developed new templates for Privacy Impact Assessment (PIA) and Contingency Planning (CP) templates in an effort to enhance VA's existing GRC tool POA&M update process.
- Conducted training on POA&Ms with system owners and data stewards on how to upload artifacts to the GRC tool
- Issued POA&M Management Guide and Authorization Requirements Standard Operating Procedures (SOP) on POA&M requirements, roles and responsibilities, escalation procedures, and update processes
- Initiated a program to further define policies and improve training to increase system owner accountability
- 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
- Incorporated POA&M requirements into the Oversight and Compliance process that will allow POA&Ms to be captured, reviewed, and reported on
- Enhanced accountability structure to manage POA&M processing through functionality within GRC workflows and procedural reviews
- Developed a cross functional compliance process for uploading POA&Ms identified during assessments where Security Control Assessment (SCA) findings are received through OCS, then vetted through the ESL Cyber Security Risk Management team prior to upload by OIS. VA is permitted 15 days to enter a response in accordance with the POA&M Management Guide

As of January 2018, the Case Management function saw an 11% decrease in the amount of open POA&Ms within its GRC tool. To support this effort, the Case Management team has coordinated with stakeholders for systems that require compliance attention. **Target Completion Date**: In Progress

Recommendation 5: We recommended the Executive in Charge for Information and technology develop mechanisms to ensure system security plans reflect current operational environments, including accurate status of the implementation of system security controls, and all applicable security controls are properly evaluated (This is a modified repeat recommendation from prior years.)

OI&T Response: VA concurs with this recommendation and will continue to enhance processes through the evolution of its Case Management POA&M and ATO action tracking, SCAs, and ESL CRM team efforts designed to perform monitoring and oversight of VA information security compliance

objectives. Through the adoption of RMF, VA will continue to enhance its workflows for routinely analyzing accreditation artifacts; including System Security Plans (SSPs), risk assessments in order for an information system to obtain an ATO. VA's GRC refresh initiatives through Fiscal Year (FY) 2018 will provide automation to support ongoing security documentation updates that will reflect the current operating environment. In addition, VA has begun planning for the deployment of a new GRC tool, which aim to utilize the various technical advances that the tool offers and provide Information System stakeholders with a solution to enhance VA capabilities and mitigate cybersecurity risks.

In addition, the Case Management teams will track action plans required of System Owners for updating required documentation as identified and escalate non-compliance to EMPD and ITOPs as required. The Case Management teams will collect, analyze, and monitor trends in information security risk across VA. The Case Management team will report, through analytical tools, the results of security compliance, vulnerability, patching, and weakness trends and areas of focus to develop a proactive strategy of meeting security objectives.

By deploying a team dedicated to working with facilities, system owners, and Information Security Officers (ISOs), Office of Information Security (OIS) will review, update, and continuously monitor security documentation in alignment with VA's policies and standards for consistent and timely updates, and sustained oversight of the security state of information systems on an ongoing basis. VA will leverage these actions to enhance the correctness of the documentation and effectively depict the operational environment of the specific system, while simultaneously maintaining consistency.

Accomplishments for this Recommendation:

- Began execution of the Case Manager function in January 2018 transitioning from activities within the Case Manager Handbook to tasks outlined within the CMPP
- Trained ISOs, System Owners, Privacy Officers, and facility staff on security artifact upload (to include Privacy Impact Assessments (PIAs) and Contingency Plans (CPs))
- Performed manual reviews of PIAs and CPs consistent with the security calendar and identified areas for enhancement
- Enhanced existing GRC functionality to support ongoing security artifact development and update process
- Further defined policies and increased training to address system owners' understanding of requirements
- Tested efforts to increase system owner accountability for the security artifact responsibilities
- Tested and reviewed SCAs for effectiveness

Organized the SCA function to align under Office of Information Security, thereby allowing oversight of SCA activities. **Target Completion Date:** In Progress

Recommendation 6: We recommended the Executive in Charge for Information and technology implement improved processes for reviewing and updating key security documents such as risk assessments, and security control assessments on an annual basis and ensure the information accurately reflects the current environment. (This is a modified repeat recommendation from prior years.)

OI&T Response: VA concurs with this recommendation and will continue to enhance processes through the evolution of its Case Management POA&M and ATO action tracking, SCAs, and ESL CRM

team efforts designed to perform monitoring and oversight of VA information security compliance objectives. Through the adoption of RMF, VA will continue to enhance its workflows for routinely analyzing accreditation artifacts; including System Security Plans (SSPs), risk assessments in order for an information system to obtain an ATO. VA's GRC refresh initiatives through Fiscal Year (FY) 2018 will provide automation to support ongoing security documentation updates that will reflect the current operating environment. In addition, VA has begun planning for the deployment of a new GRC tool, which aim to utilize the various technical advances that the tool offers and provide Information System stakeholders with a solution to enhance VA capabilities and mitigate cybersecurity risks.

In addition, the Case Management teams will track action plans required of System Owners for updating required documentation as identified and escalate non-compliance to EMPD and ITOPs as required. The Case Management teams will collect, analyze, and monitor trends in information security risk across VA. The Case Management team will report, through analytical tools, the results of security compliance, vulnerability, patching, and weakness trends and areas of focus to develop a proactive strategy of meeting security objectives.

By deploying a team dedicated to working with facilities, system owners, and Information Security Officers (ISOs), Office of Information Security (OIS) will review, update, and continuously monitor security documentation in alignment with VA's policies and standards for consistent and timely updates, and sustained oversight of the security state of information systems on an ongoing basis. VA will leverage these actions to enhance the correctness of the documentation and effectively depict the operational environment of the specific system, while simultaneously maintaining consistency.

Accomplishments for this Recommendation:

- Began execution of the Case Manager function in January 2018 transitioning from activities within the Case Manager Handbook to tasks outlined within the CMPP
- Trained ISOs, System Owners, Privacy Officers, and facility staff on security artifact upload (to include Privacy Impact Assessments (PIAs) and Contingency Plans (CPs))
- Performed manual reviews of PIAs and CPs consistent with the security calendar and identified areas for enhancement
- Enhanced existing GRC functionality to support ongoing security artifact development and update process
- Further defined policies and increased training to address system owners' understanding of requirements
- Tested efforts to increase system owner accountability for the security artifact responsibilities
- Tested and reviewed SCAs for effectiveness

Organized the SCA function to align under Office of Information Security, thereby allowing oversight of SCA activities. **Target Completion Date**: In Progress

Recommendation 7: We recommended the Executive in Charge for Information and technology implement mechanisms to enforce VA password policies and standards on all operating systems, databases, applications, and network devices. (This is a repeat recommendation from prior years.)

OI&T Response: VA concurs with this recommendation that standardized processes are required to enforce password policy and security configuration baselines. VA is currently taking measures to address the findings regarding service account password configuration and the service account password change

process. VA plans to implement the current Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Privileged Account Management (PAM) from the initial Information Operations (IO) data center implementation along with long term integration with CDM CyberArk throughout VA. The implementation of this solution will consist of three phases: phase one will address local administrator accounts, phase two will address system service accounts, and phase three will address enterprise and domain administrator accounts. The CDM PAM CyberArk solution will provide PAM auditing and access control for service accounts throughout VA. One of the future capabilities of the CDM PAM CyberArk solution will be to track the password life cycle of service accounts in an automated process to remediate the associated findings.

Accomplishments for this Recommendation:

- Implemented a 2.5 yearly service accounts Action Item (AI) process to address service account password changes, which is tracked by Infrastructure Operations using Secret Server
- Utilizing CyberArk Discover and Audit (DNA) capabilities and DBNetwork DB user discovery to identify and create an inventory of service accounts, which will allow for password tracking through the CyberArk PAM solution.

Target Completion Date: In Progress.

Recommendation 8: We recommended the Executive in Charge 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 As a result of the Field Security Service (FSS) Transformation, the Office of Information and Technology (OI&T) established a Cyber Security Risk Management Team. This team will standardize the auditing of generic and inactive accounts to enforce compliance. The team is accountable for monitoring generic, inactive and password management reviews, developing guidelines to monitor user accounts for Active Directory, VistA and Common Security Service (CSS) systems, delivering a series of Webinars to educate the Information Security Officer (ISO) community on how to properly conduct, documenting and testing the account management security controls in place.

VA is working with the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program to implement efforts to create a master user record (MUR). The MUR will be a record for users with access to the VA network. The MUR will integrate with CyberArk for managing privileged access to VA networks. The integration will provide provisioning services, de-provisioning services and support access certification of privileged access. Initial development efforts with CDM will begin in the third quarter of FY18. Community Care Transformation Fee Basis Claims System (FBCS) Project Manager (PM) will work with the Claims, Adjudication and Reimbursement (CAR) organization to map out a process to perform reviews of personnel access inside of FBCS to coincide with VistA fee access Reviews. Additionally, the Community Care Transformation FBCS PM will work with the local Business Implementation managers to implement the same process. Target Date of Completion is December 2017.

Accomplishments for this Recommendation:

- VA implemented a Security Control Assessment (SCA) capability to audit user access rights in November 2016.
- The development and delivery of a series of mandatory Webinars (6) to educate the ISO community on how to properly conduct, document and test the account management security controls in place: Auditing Essentials, Account Management Functions, Elevated Privileges Reviews and Programmer Mode Access/Functions, Separated Users and Sensitive Records Review, Wireless Connectivity and Sanctuary Access, and FileMan Menu Audit and VistA/Veternas Benefit Administration (VBA) Users Access Review.

    - The first Information Security Webinar to focus on Auditing Essentials was conducted on October 16, 2017 with 176 professionals in attendance.

Requirements elaboration discussions began in FY17 and the initial development efforts for CDM will begin in the third quarter of FY18. **Target Completion Date:** In Progress

Recommendation 9: We recommended the Executive in Charge 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 partial non-concur. OIG reported that "security logs were not effectively managed or proactively reviewed. Specifically, we noted that the Splunk tool was implemented for enhanced audit log analysis within Field Operations and the NSOC TIC gateways. However, the system only collected logs from Windows servers, Linux servers, and network infrastructure devices. Other systems such as VistA, the Veteran's Service Network (VETSNET), and the Veteran's Benefits Management System (VBMS) were not incorporated into the enhanced audit log monitoring and security event correlation process."

Splunk and the Security Information and Event Management (SIEM) tool effectively manage security logs which are proactively reviewed for suspect and or malicious activity. The SIEM environment is configured to receive, correlate, and act upon data that traverse each of VA's TICs, which includes traffic associated with VistA, the Veteran's Service Network (VETSNET), and the Veteran's Benefits Management System (VBMS).

If the OIG has identified specific application related logs that OIG believes should be directly logged to the Splunk environment, this specific information should be conveyed to the Application System Owner for review and consideration. At this time, the NSOC's Centralized logging repository is collecting system, application, and infrastructure logs that VA system owners have authorized. This finding may still be an Enterprise-Wide Weakness, but it would be associated with the application, not the NSOC's SIEM environment, as the SIEM is capable and prepared to receive these logs, however at this time NSOC has not been authorized by the respective system owners to collect and act upon this data. VA will continue to improve system owner accountability and communication with NSOC to ensure that audit logging for critical systems is performed.

OIG reported that "certain privileged functions within VistA such as "EVE" and "Postmaster" were not reviewed for appropriate permissions. Privileged functions were logged within VistA, but there was no process in place to review the actions for malicious and suspicious activity." However, this is an

application-related finding and should be tied to the application, not be directly tied to the Enterprise SIEM. Furthermore, the OIG reported that domain controller audit logs were not retained for a minimum of one year as required by VA Handbook 6500. However, Domain Controller logs are collected into the Enterprise SIEM and retained for a minimum of one year. **Target Completion Date:** In progress.

Recommendation 10: We recommended the Executive in Charge 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 that two-factor authentication should be fully implemented in remote and local system access throughout VA. The IO data center IT security infrastructure standard Security Threat Module (STM) addresses IT Security threats to the following systems: Terminal Access Controller Access Control System, Structured Query Language, Oracle, Linux, Veterans Health Information Systems and Technology Architecture (VistA), OpenVMS, Cache, Microsoft Windows, Burial Operations Support System/Automated Monument Application System, and Mainframe. These systems primarily reside in the IO data centers where the security STM standards exist. STM provides mitigation for the current risk of user accounts becoming exploited, thereby preventing unauthorized access to application resources without proper user accountability. The purpose of STM is to provide interim mitigation to applications that do not currently have two-factor authentication enforced. The various solutions within the STM tool (i.e., malware protection, intrusion prevention, web application firewall, privileged account management and Security Information and Event Monitoring (SIEM) threat correlation analysis) protect the VA applications against potential malicious activity.

VA has also implemented two-factor authentication for administrator user accounts across IO. VA is making use of CyberArk DNA capabilities and DBNetwork DB user discovery to identify and create an inventory of service accounts. This will allow CyberArk PAM to associate the existing two-factor authentication administrator account to the service account with user auditing and user restrictions. These restrictions will only allow configured access between two-factor authorization administrators, service accounts and specific systems mapped for the access. In addition, VA is currently at 80% compliance in regards to applications with Personal Identity Verification (PIV) enabled two-factor authentication, and are pushing for a Kernal patch to be released which will bring the compliance up to 90%. VA's Centrify project will enable PIV centralization of all non-Microsoft systems into one enterprise authentication configuration, which is currently VA's Active Directory (AD).

Accomplishments for this Recommendation:

- Utilized CyberArk DNA capabilities and DBNetwork DB user discovery to identify and create an inventory of service accounts allowing the CyberArk PAM solution to associate the existing two-factor authentication administrator accounts to the service accounts
- Enforced two-factor authentication 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)
- Required use of Personal Identity Verification (PIV) card to authenticate at the gateway
- Implemented a process for the National Service Desk (NSD) to provide a temporary exemption from two-factor authentication in emergency situations.

Target Completion Date: In Progress

Recommendation 11: We recommended the Executive in Charge 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 Partial Non-Concur. The OIG stated that "VA did not perform credentialed scans on all systems on the network. The NEWT tool reported that VA had conducted scans for many of its systems without using system security credentials. Using credentialed security scans will provide a more complete listing of system and application vulnerabilities. Consequently, VA's remediation efforts were not effective in addressing all security vulnerabilities on systems included within their scanning processes. Overall, we noted that the number of devices included within credentialed security scans has improved compared to the prior year. VA's Enterprise Predictive Scanning process evaluated certain medical devices for security issues but this process did not address the security vulnerabilities during its remediation efforts. Moving forward, this process needs to evaluate and remediate security weaknesses for medical devices that are connected to the general network and not isolated by MDIA."

It is more correct to state that not each of the scanned systems returned authenticated results. For the past three years VA has proactively addressed this issue. VA has worked with region personnel to implement our scanning credentials on all major Operating Systems (OS) across the enterprise. The number of credential failures has decreased as we work through this project (as noted by the OIG). We continue to work with region personnel to address those instances where we observe credential failures.

The NSOC has developed and implemented a documented review and troubleshooting process to detect instances where network segments did not return expected results. The NSOC and NEWT Team have jointly developed an Authentication Gap Analysis Dashboard to identify and address specific systems/devices where authentication failures occurred. Additionally, we have developed and implemented processes and tools to determine the security posture of systems/devices where the Nessus scanning tool does not provide a thorough assessment or where results can be enhanced.

In regards to remediating deficiencies, in January 2017 VA implemented the VA Flaw Remediation process outlined in the VA Flaw Remediation SOP which addresses critical, high, moderate, low, and emergent remediation needs. VA continues to refine and improve this process with the establishment of the Vulnerability Management Program office under the CISO's direction.

The OIG stated "VA's Network Security Operations Center (NSOC) does not have a comprehensive inventory of the agency's systems for scanning because the NSOC local scanner is placed in a network range that differs from the local network range used by the facilities for network monitoring. In addition, the NSOC did not have system credentials to access all computer and network devices for scanning. Regarding systems not managed by OI&T, we noted numerous security vulnerabilities that were not addressed by system owners in a timely manner. VA has not implemented effective methodologies for monitoring medical devices on the general network and ensuring such devices are segregated from the local area network."

The NSOC requests clarification on the statement "VA's Network Security Operations Center (NSOC) does not have a comprehensive inventory of the agency's systems for scanning because the NSOC local scanner is placed in a network range that differs from the local network range used by the facilities for network monitoring." VA has over 300 scanners deployed across each region in the enterprise. These scanners are located on the local network and behind the firewall of facilities within these regions.

Accomplishments for this Recommendation:

- Improved metrics on critical vulnerabilities
- Maintained a master list of vulnerability scan types and frequencies
- Implemented monthly Cisco network device compliance scanning
- Implemented monthly Red Hat Enterprise Linux (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
- Enhanced NEWT to capture documentation of remediation performed
- Implemented an improved patch and vulnerability management process
- 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 authenticated scan processes
- Completed enterprise credentialed Mac, other Unix/Linux OS, network, and other devices scan process testing
- Implemented credentialed Mac, other Unix/Linux OS, network, and other devices authenticated scan processes
- Performed gap analysis of devices not providing credentialed scans
- Collaborated with System Owners to remediate scanning issues to receive credentialed scans

Developed the Printer Assessment process (see supporting documentation embedded above), DbProtect deployment for enterprise wide Database scanning, the Enterprise Discovery Scan (combines automated and manual assessment of ports and services), and OS Targeted Scans. **Target Completion Date**: In Progress

Recommendation 12: We recommended the Executive in Charge 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. Infrastructure Operations Security Management office is responsible for directing the agency Vulnerability Management program per the Enterprise Cybersecurity Strategy Update: Enterprise Vulnerability Management memorandum released on June 30th, 2017. IO Security Management has initiated projects to address gaps in vulnerability scanning and credential management, strengthen and standardize patch and vulnerability management practices across the enterprise. The Vulnerability Management program is also leading targeted efforts pertaining to management of risk inherent to medical devices, SPS's, web applications and databases which encompass a significant percentage of the VA technology footprint and are valuable to operations and service delivery.

Accomplishments for this Recommendation:

IO Security Management has established and staffed the Vulnerability Management Program office in response to the CISO memorandum Vulnerability Management program. **Target Completion Date:** In Progress

Recommendation 13: We recommended the Executive in Charge for Information and technology maintain complete and accurate baseline configurations for all platforms 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. VA has defined processes and controls for implementing enterprise baseline configurations by actively using its existing Continuous Readiness in Information Security (CRISP) Baseline SOP for security control Configuration Management-2 (CM-2) requirements. VA modified the baseline SOP to strengthen the baseline process and include provisions to review and modify baselines according to an established schedule. VA implements the process for change and configuration management as identified in National Institute of Standards and Technology (NIST) 800-53a Rev 3. Related controls include: CM-3, CM-6, CM-8, CM-9, System and Services Acquisition-10 (SA-10), Program Management-5 (PM-5), PM-7.

VA continues to develop reports for monitoring baseline compliance in the IBM BigFix, System Center Configuration Manager (SCCM), Microsoft Configuration Manager, and VA-developed NEWT and LADDER reporting systems following DISA STIGs and United States Government Configuration Baseline (USGCB) settings.

VA uses the System Engineering Design Review (SEDR) to review configuration management processes. The National Change Configuration Board (NCCB), which follows requirements outlined in the VA Enterprise Change Control Policy, approves configuration management processes. Once a baseline is approved, it is posted to the VA SharePoint repository for approved baselines. With the new process using the Service Desk Management (SDM) tool, change management module, VA will have a change order for each baseline review that tracks the review from start date to completion date. When updates are required of a VA baseline out of the review the workflow will automatically route requirements to the Solution Delivery Engineering team responsible for proper action and track changes until approved and published on the VA Baseline portal for field implementation.

Where a baseline does not have automated scanning capabilities due to technology limitations, VA will implement a formal manual review process. Once deviations are identified, the system owner and information security officers are directed to record them as Plan of Action and Milestones (POA&M), per VA 6500 requirements. System owners should determine if systems adhere to the approved VA Baseline prior to bringing the systems online in the production environment.

In order to address the Federal Information Security Measurement Act (FISMA) Material Weakness associated with this metric, departments under the Office of Information and Technology (OI&T) are standing up a follow on project to Enterprise Cybersecurity Strategy Team (ECST) Plan of Action (POA) 17 project in order to further mature the configuration baseline process. The project is expected to be scoped to improve existing processes for intake, development, testing, implementation, and compliance monitoring for new baselines. The project is expected to address current approved baseline documents, with OI&T performing a review of baselines, developing the compliance reports utilizing existing

reporting tools such as IBM BigFix, Microsoft Configuration Manager, and VA-developed NEWT and Log Analysis Distributed Database Enterprise Reporting (LADDER) reporting systems.

The estimated Project Roadmap for Maturing Configuration Baselines throughout FY2018 can be found below:

- Documenting process improvements though new standard operating procedures – April 30, 2018
- Implementing process improvements – June 30, 2018
- Review of approved baselines to document and design the compliance checklist
    - 50% completion of review and compliance reports available – April 30, 2018
    - 80% completion of review and compliance reports available – August 30, 2018

The remaining 20% estimated will require manual monitoring due to technology limitations or may require VA to divest the technology and replace it with new technology. Recommendations for the final 20% are required by September 30, 2018

Accomplishments for this Recommendation:

- Performed review and update of currently published baselines
- Developed and published an improved SOP for baseline updates
- Enhanced existing tool to provide Cisco network device baseline configuration monitoring across VA
- Examples of efforts since the conclusion of the FY2017 OIG audit season include, new reporting for compliance with new approved Redhat Linux version 7 Baseline
- OI&T also has received new baseline request to develop VA Baseline configuration for platforms on the VA network
- Began tracking baseline development on 22 new VA baseline configurations, with 18 being approved and the list of new baselines continuing to expand until VA has properly documented baselines for active technologies on VA networks

Developed and implemented an automated formal recording of annual reviews conducted on newly approved baselines. For existing VA baselines, the process will be implemented at the time of the required annual review. **Target Completion Date:** In Progress

Recommendation 14: We recommended the Executive in Charge for Information and technology improved network access controls to ensure medical devices and networks, not managed by OIT, are appropriately segregated from general networks and mission-critical systems. (This is a repeat recommendation from prior years.)

OI&T Response: VA Concurs. The VA's Medical Device Protection Program (MDPP) and Veterans Health Administration (VHA) implemented the Enterprise Cyber Security Team (ECST) Medical Cyber (MedCyber) Domain in response to the Material Weakness identified during the FY15 Office of the Inspector General (OIG) Federal Information Security Modernization Act Audit (FISMA). In FY17 the MedCyber team developed and implemented processes to further address security weaknesses and improve the VA's security posture. VA's MDPP/MedCyber has accomplished the following:

• Since the initial deployment of the VHA Healthcare Technology Management's Networked Medical Device Database (NMDD), tools have been developed that allow for improved visibility of network-attached medical equipment in a more automated manner. All medical devices connected to the VA network and behind a Medical Device Isolation Architecture (MDIA) Access Control List (ACL) will be automatically inventoried by VA's Network and Security Operations Center (NSOC) and placed into a report that downloads to NMDD for use by the Biomedical Engineering staff. Key technical attributes of network-attached medical equipment are then automatically inputted into the NMDD after validation by Biomedical Engineering staff.

• In support of the March 2016 VHA memo prohibiting the purchase of medical devices with unsupported operating systems, in VHA has improved the security posture of network-connected medical devices by reducing the inventory with unsupported OS by 37% since April 2016.

• In FY17 VA's remediation of ACLs with the highest security aperture ratings (which are a relative measure of the # of open ports) increased the security posture of the MDIA Program by 98%. In a cross-organizational effort, the 'MDIA ACL External Security Aperture Metric' was implemented to reduce unnecessary broad port ranges. The metric is now used to score the external connection security posture of all VA facilities containing components of the Medical Device Isolation Architecture.

• Continuous monitoring of each of the 16,000+ MDIA ACLs was a manual, labor-intensive process that took the entire year to complete. Each ACL could only be scored a single time during the period, and remediation actions were based on this single snapshot. In order to improve upon this methodology, the MedCyber Team, in conjunction with Network Security Operations Center (NSOC) staff, is developing an automated process that allows for daily scoring of every MDIA ACL against the MDIA ACL Ruleset. These daily scores and detailed information about ruleset violations have been integrated into the VA NSOC's Log Analysis and Distributed Database Enterprise Reporting (LADDER) tool for ready access and prompt remediation. Full deployment of the automated MDIA ACL review will be in FY18.

• Through the MDIA ACL automated review efforts, VA has been able to identify, remove, and/or correct ACLs to the proper interfaces. This improves the visibility and data gathering of MDIA ACL information and medical device inventory. Since this step began in May 2017, the number of ACLs not properly applied to interfaces has decreased by 78%.

• In parallel to working enhancements to the MDIA, Field Security Services (FSS) HISD is pursuing a future isolation architecture solution leveraging new technology, called MedFusion. The team will build on the success of the MDIA and will benefit from the efficiencies of the new technology.

• A workgroup led by the MedCyber Project Managers authored a whitepaper document that summarizes vendor demonstrations and provides good/better/best analysis, both as an Integrated Master Schedule (IMS) deliverable and as a reference for providing Leadership with decision making support for selecting options to address the "Securing Medical Devices and the Internet of Things (IoT)". The workgroup successfully completed documentation for three Requests for Information (RFI), orchestrated eight face-to-face vendor demonstrations, completed a Request for Proposal (RFP), completed an evaluation of responses, and was awarded a contract for the MedFusion workgroup's appliance-based isolation solution on 9/25/2017.

Accomplishments for this recommendation:

- Implemented tools that leverage the NSOC's report of network-connected medical devices to improve the NMDD network-attached medical device inventory in a more automated manner.
- Reduced the number of network-connected medical device with unsupported operating systems by 37% from April 2016 to October 2017.
- Remediated MDIA ACLs with the highest security aperture ratings which increased the security posture of the MDIA Program by 98%.
- Developed automation of the MDIA ACL review process which will provide more timely and frequent reviews and will standardized the reviews creating a more efficient and higher quality approach.

Identified, removed, and/or corrected ACLs to the proper interfaces. Since May 2017 the number of ACLs not properly applied to interfaces has decreased by 78%. **Target Completion Date:** In Progress

Recommendation 15: We recommended the Executive in Charge for Information and technology consolidate the security responsibilities for networks, not managed by OIT, 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. In response to the Material Weakness identified during the FY17 Office of the Inspector General (OIG) Federal Information Security Modernization Act Audit (FISMA), VA continues to address the security issue outlined above.

The Department of Veterans Affairs (VA) Health Information Security Division (HISD) and Veterans Health Administration (VHA) have implemented a process to address device vulnerabilities on local facility systems not managed by OI&T. Medical device and Special Purpose System cybersecurity are 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, facility management, 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 confirmed 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.
• Each VHA facility has performed a Risk Analysis to document the compensating controls related to devices that cannot follow VA baseline guidance.

Accomplishments for this recommendation:

- VA O&IT has accepted responsibility for devices connected to the VA network through the issuance of policy that required networked connected devices, tenant networks and medical devices to be accounted for as part of the existing General Support System, making the system owner responsible for devices connected to the VA network in their system boundary area or responsibility.
- Developed System Assignment Process filter within NEWT to track medical device vulnerabilities and assign resources to the remediation of those vulnerabilities.
- Developed an enterprise-wide Special Purpose Systems Program, which includes inventory, vulnerability and incident management program for Network-connected non-medical, non-traditional IT systems.
- Established a database to identify Special Purpose Systems and their system owners throughout the VA enterprise. Data gathered is compiled into a SPS database, which greatly increases the efficiency in which the VA can respond to identified threats.
- Created and implemented a Standard Operating Procedure to systematically address cyber security risks on SPS Network-connected devices identified by the VA's Enterprise vulnerability scanners.
- Opened POA&M's for medical devices running an unsupported Operating System and where the vendor of the medical device has not confirmed the installation / implementation of remediation steps. This is being tracked within the GRC tool.

Opened POA&M's for Special Purpose Systems running an unsupported Operating System and where the vendor of the device has not confirmed the installation / implementation of remediation steps. This is being tracked within the GRC tool. **Target Completion Date:** In Progress

Recommendation 16: We recommended the Executive in Charge for Information and technology implement improved processes to ensure that all devices and platforms are evaluated using credentialed vulnerability assessments. (This is a repeat recommendation from prior years.)

OI&T Response: VA Partially Non-Concurs. The OIG stated that "VA did not perform credentialed scans on all systems on the network. The NEWT tool reported that VA had conducted scans for many of its systems without using system security credentials. Using credentialed security scans will provide a more complete listing of system and application vulnerabilities. Consequently, VA's remediation efforts were not effective in addressing all security vulnerabilities on systems included within their scanning processes. Overall, we noted that the number of devices included within credentialed security scans has improved compared to the prior year. VA's Enterprise Predictive Scanning process evaluated certain medical devices for security issues but this process did not address the security vulnerabilities during its remediation efforts. Moving forward, this process needs to evaluate and remediate security weaknesses for medical devices that are connected to the general network and not isolated by MDIA."

It is more correct to state that not each of the scanned systems returned authenticated results. For the past three years VA has proactively addressed this issue. VA has worked with region personnel to implement our scanning credentials on all major Operating Systems (OS) across the enterprise. The number of credential failures has decreased as we work through this project (as noted by the OIG). We continue to work with region personnel to address those instances where we observe credential failures.

The NSOC has developed and implemented a documented review and troubleshooting process to detect instances where network segments did not return expected results. The NSOC and NEWT Team have jointly developed an Authentication Gap Analysis Dashboard to identify and address specific systems/devices where authentication failures occurred. Additionally, we have developed and implemented processes and tools to determine the security posture of systems/devices where the Nessus scanning tool does not provide a thorough assessment or where results can be enhanced.

In regards to remediating deficiencies, in January 2017 VA implemented the VA Flaw Remediation process outlined in the VA Flaw Remediation SOP which addresses critical, high, moderate, low, and emergent remediation needs. VA continues to refine and improve this process with the establishment of the Vulnerability Management Program office under the CISO's direction.

The OIG stated "VA's Network Security Operations Center (NSOC) does not have a comprehensive inventory of the agency's systems for scanning because the NSOC local scanner is placed in a network range that differs from the local network range used by the facilities for network monitoring. In addition, the NSOC did not have system credentials to access all computer and network devices for scanning. Regarding systems not managed by OI&T, we noted numerous security vulnerabilities that were not addressed by system owners in a timely manner. VA has not implemented effective methodologies for monitoring medical devices on the general network and ensuring such devices are segregated from the local area network."

The NSOC requests clarification on the statement "VA's Network Security Operations Center (NSOC) does not have a comprehensive inventory of the agency's systems for scanning because the NSOC local scanner is placed in a network range that differs from the local network range used by the facilities for network monitoring." VA has over 300 scanners deployed across each region in the enterprise. These scanners are located on the local network and behind the firewall of facilities within these regions (see supporting documentation embedded below).

Accomplishments for this Recommendation:

- Improved metrics on critical vulnerabilities
- Maintained a master list of vulnerability scan types and frequencies
- Implemented monthly Cisco network device compliance scanning
- Implemented monthly Red Hat Enterprise Linux (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
- Enhanced NEWT to capture documentation of remediation performed
- Implemented an improved patch and vulnerability management process
- 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 authenticated scan processes
- Completed enterprise credentialed Mac, other Unix/Linux OS, network, and other devices scan process testing
- Implemented credentialed Mac, other Unix/Linux OS, network, and other devices authenticated scan processes
- Performed gap analysis of devices not providing credentialed scans

- Collaborated with System Owners to remediate scanning issues to receive credentialed scans

Developed the Printer Assessment process (see supporting documentation embedded above), DbProtect deployment for enterprise wide Database scanning, the Enterprise Discovery Scan (combines automated and manual assessment of ports and services), and OS Targeted Scans. **Target Completion Date:** In Progress

Recommendation 17: We recommended the Executive in Charge 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. VA deployed measurable processes and controls for implementing configuration change control activities by using established standard operating procedures (SOPs) and policies. The records of configuration controlled changes follow a standardized method of the following:

- Performing a technical review
- Security assessments
- Scheduling
- Approval
- Implementation
- Verification of the implemented changes

Additionally, VA retains these records within the VA Approved Change Management System. VA established change control boards, which provide coordination, oversight, and approval to changes that are high priority, high impact, high risk, and require downtime, as defined in the National Change Management Process SOP. VA established quarterly audits, which sample changes in the Change Management System to confirm the changes meet required processing. Changes that do not follow policy are escalated to management for resolution. VA is implementing a new service management tool,Service Now2, that is expected to further improve the auditing and reporting capability for changes in the future.

Accomplishments for this Recommendation:

- Established change control boards to provide oversight and approval of high priority, high risk, and high impact system changes

Implemented Service Now2 as a new service management tool expected to improve future auditing and reporting capabilities. **Target Completion Date:** In Progress

Recommendation 18: We recommended the Executive in Charge 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 and is aware of the systemic risk associated with unencrypted legacy Microsoft Exchange backup data. We consider the risk associated with this finding to be adequately managed with our compensating controls and will be documented in the risk

management framework. This is also a prior-year recommendation noted in the Fiscal Year (FY) 2016 FISMA audit report. There is no plan to encrypt legacy Microsoft Exchange backup tapes, due to VA's migration to a Microsoft Office 365 cloud solution. Instead, Enterprise Systems Engineering created Plans of Action and Milestones (POA&M) that would decommission legacy Microsoft Exchange backup tapes at VA sites and developed a contract to securely transport tapes to a third party site for storage and restoration services.

Currently, there are seven (7) sites using the same third party vendor for secure storage of their Microsoft Exchange backup tapes. The contract includes the seven (7) sites and fourteen other Microsoft Exchange facilities that store backup tapes in local facilities. This consolidation will fall under VA's current POA&M that allows for the secure shipping of the unencrypted tapes. Once moved, the vendor will provide restoration services from the tapes as requested and return it to VA on encrypted hard drives. The third party contract for VA Legacy Tape Storage and Legacy Tape Restoration was awarded on September 26, 2017.

Accomplishments for this Recommendation:

- Released a series of National Action Items (NAIs) to field offices for identifying systems and applications that use backup tapes as their method for offline storage, as well as non-compliant sites transferring unencrypted backup tapes offsite for storage.
- Developed Standard Operating Procedures (SOP) to apply standards and leading practices developed within VA to define tape backup retention policies, a data loss mitigation strategy, and disaster recovery and data protection standards for an enterprise-wide backup strategy.

Procured third party vendor contract to collect and consolidate unencrypted Microsoft Exchange backup tapes for the purpose of storage and restoration services**. Target Completion Date:** In Progress

Recommendation 19: We recommended the Executive in Charge 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 the assigned sites and within stated timeframes. (This is a modified repeat recommendation from prior years.)

OI&T Response: VA concurs with this recommendation and will implement improved processes for testing of contingency plans (CPs) and failover capabilities for financial applications and general support systems to confirm that critical components can be recovered at an alternate site in the event of a system failure or disaster.

VA has implemented annual processes to update Information System Contingency Plans (ISCPs) are updated with the required information (e.g., contingency plans, disaster recovery plans, and business impact analysis). Additional steps will be taken to confirm system owners are reviewing and updating 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. Each year, Information Technology Operations and Services (ITOPS) provides guidance to area managers, ISOs, and technical subject matter experts 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). Disaster Recovery (DR) / Continuity of Operations (COOP) supervisors review draft plans for operational feasibility and provide feedback as to whether plans are

compliant with VA and National Institutes of Standards and Technology (NIST) guidance. Following review and approval (pending required changes) of contingency plans by ITOPS, the system owner signs the plan and uploads to the Governance Risk and Compliance tool.

OI&T has employed a resilient infrastructure designed to minimize the impact of disruption to Mission Essential Functions. This includes a strategy to recover and perform system operations at an alternate facility for an extended period. OI&T has proven that it has the ability and expertise to successfully recover systems and move systems between facilities and datacenters without a single failure and within the prescribed Recovery Time Objective (RTO) by conducting multiple VistA migration between data centers.

ITOPS will work with VA security stakeholders to update existing policy to reflect changes in our operational environment and organizational structure to reflect the improvements gained in the management and oversight of these systems. During the FY18 ISCPA planning cycle, Appendix D: Recovery Site in the ISCP plans will be updated to reflect the current organizational structure for systems that would be recovered in place. Recovery Site will also be updated to identify systems current recovery site since moving to an Infrastructure Operations (IO). Testing in FY18 cycle will continue to be focused on Enterprise testing. When creating the testing scenarios ITOPS will ensure that recovery at alternate site listed in Appendix D is tested (i.e., tabletop exercises and functional testing from backed up media). VA considers this simulated production environment that adequately represents the requirements for failover testing is balanced against preservation of mission critical business continuity.

Accomplishments for this Recommendation:

- Conducted a compliance review and assessment of approximately 720 FY17 CPs and DR plans.

Developed the Enterprise Testing SOP to test the Enterprise escalation and response capabilities. **Target Completion Date:** In Progress

Recommendation 20: We recommended the Executive in Charge 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. VA conducted an inventory of VA sites to identify external connections on an ongoing basis and as new connections are reported. Validation of each identified connection occurs when the connection has been reported. Non-compliant connections will be migrated to the VA Trusted Internet Connection (TIC) Gateways and decommissioned thereafter. In addition, non-compliant connections are expected to be brought under the control of NSOC Security Configuration Services (SCS) with the deployment of an Intrusion Prevention System (IPS) to the site(s). The Enterprise Security Change Control Board (ESCCB) is currently working with Business Partner Gateway (BPG) owners to become TIC compliant.

The VA NSOC Compliance Scanning Services (CSS) Team monitors contractor-hosting facilities' connections, which fulfills continuous monitoring requirements for VA systems hosted outside the VA network with the use of the internal Tenable Security Center Console method to communicate with remote scanners established inside business partner networks. This connections monitoring is expected

to be expanded to new remote Business Partners. Their remote Internet Protocol (IP) will be a function of the business partner's network and unknown to the CSS team until the remote scanner is configured.

Additionally, VA published VA Directive and Handbook 6513, Secure External Connections, governing the process for managing and continuously monitoring VA connections in October 2017.

Accomplishments for this Recommendation:

- Reviewed 1,500+ site responses noting external interconnections at the responding sites
- Confirmed mechanism(s) 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
- Performed telecommunication closet review of external connections
- Enforced Trusted Internet Connection 2.0 compliance
- Held transition meetings with Facility Chief Information Officers (FCIO), system owners, business partners, and Information Security Officers (ISOs) for newly identified noncompliant connections from the November 2015 Action Item

Published Directive and Handbook 6513, Secure External Connections, governing the process for managing and continuously monitoring VA connections. **Target Completion Date:** In progress.

Recommendation 21: We recommended the Executive in Charge 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. The VA Network and Security Operations Center (NSOC) initiated a Cyber Incident Response Working Group (IRWG) in March 2014, to improve VA's Incident Response capability. The working 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 working 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 the VA NSOC, Information Security Officers (ISOs), and Information Technology Operations and Services (ITOPS) to facilitate situational awareness on open tickets and their remediation progress.

The 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 to include identified incidents are remediated in a timely manner and a Federal Information Security Modernization Act (FISMA) requirement to track enterprise-wide metrics for incident response. From FY 15 – FY17, the average incident ticket closure time was reduced from 22 days to 6.78 days. In addition, in FY16, the VA NSOC implemented containment of cyber security threats, which isolates the system from the network until the threat has been removed. During FY17, the average containment of a cyber security threat was less than 24 hours effectively reducing threats to VA. The VA NSOC continues to

develop new processes and tracking of metrics to strengthen the agency-wide incident response process.

Accomplishments for this Recommendation:

- Implemented new Security Incident Response policies and plans in an updated NSOC Incident Response Plan
- 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 role

Reduced time to containment and time to closure of incident response tickets. **Target Completion Date:** In progress.

Recommendation 22: We recommended the Executive in Charge 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 repeat recommendation from prior years.)

OI&T Response: VA Partial Non-Concur. OIG reported that "security logs were not effectively managed or proactively reviewed. Specifically, we noted that the Splunk tool was implemented for enhanced audit log analysis within Field Operations and the NSOC TIC gateways. However, the system only collected logs from Windows servers, Linux servers, and network infrastructure devices. Other systems such as VistA, the Veteran's Service Network (VETSNET), and the Veteran's Benefits Management System (VBMS) were not incorporated into the enhanced audit log monitoring and security event correlation process."

Splunk and the Security Information and Event Management (SIEM) tool effectively manage security logs which are proactively reviewed for suspect and or malicious activity. The SIEM environment is configured to receive, correlate, and act upon data that traverse each of VA's TICs, which includes traffic associated with VistA, the Veteran's Service Network (VETSNET), and the Veteran's Benefits Management System (VBMS).

If the OIG has identified specific application related logs that OIG believes should be directly logged to the Splunk environment, this specific information should be conveyed to the Application System Owner for review and consideration. At this time, the NSOC's Centralized logging repository is collecting system, application, and infrastructure logs that VA system owners have authorized. This finding may still be an Enterprise-Wide Weakness, but it would be associated with the application, not the NSOC's SIEM environment, as the SIEM is capable and prepared to receive these logs, however at this time NSOC has not been authorized by the respective system owners to collect and act upon this data. VA will continue to improve system owner accountability and communication with NSOC to ensure that audit logging for critical systems is performed.

OIG reported that "certain privileged functions within VistA such as "EVE" and "Postmaster" were not reviewed for appropriate permissions. Privileged functions were logged within VistA, but there was no process in place to review the actions for malicious and suspicious activity." However, this is an

application-related finding and should be tied to the application, not be directly tied to the Enterprise SIEM. Furthermore, the OIG reported that domain controller audit logs were not retained for a minimum of one year as required by VA Handbook 6500. However, Domain Controller logs are collected into the Enterprise SIEM and retained for a minimum of one year. **Target Completion Date:** In progress.

Recommendation 23: We recommended the Executive in Charge 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 repeat recommendation from prior years.)

OI&T Response: VA Concurs. VA is researching several alternatives to address the identification and prevention of unauthorized scans through the deployment of additional intrusion detection sensors and event correlation. VA is in the process of baselining traffic from devices utilized at medium and large facilities across VA. VA plans to continue refining the capability within the enterprise Security Information and Event Management (SIEM), to more effectively correlate source and destination event patterns to identify "unauthorized" scanning activity, which occurs when authorized scanners scan hosts outside of a perceived yet undisclosed scan boundary.

Accomplishments for this Recommendation:

- Modified internal event correlation process to help identify scans outside of the scan boundaries

Procured and deployed next generation application firewall solution, Palo Alto PAN 7080, at TIC gateways in the first quarter of FY 17. **Target Completion Date:** In progress.

Recommendation 24: We recommended the Executive in Charge 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. VA uses the Technical Reference Model (TRM) site to present a list of assessed technologies and standards used to develop, operate, and maintain enterprise applications. Software not classified within TRM is considered "unmanaged". A team of analysts works through the backlog of unmanaged software currently installed on the network, utilizing available tools (e.g., BDNA, System Center Configuration Manager (SCCM), TRM, Google, Security Management and Analytics (SMA) Vulnerability reports) to prioritize and analyze these titles and submit to TRM for review and classification. Additionally, the team surveys VA's network of end-users to determine the business need for software technologies prior to submission to TRM.

While VA does not have a fully developed and implemented software "Whitelist" of approved software for use on the VA network, VA does have an active and funded project to develop and implement a Blacklist of software that is not approved for use on the VA network. The Blacklist project focuses on the deployment of the Continuous Diagnostics and Mitigation (CDM) Software Asset Management (SWAM) capability and is part of a larger CDM deployment effort in collaboration with the Department of Homeland Security (DHS). Following NIST guidelines, VA will "prevent the execution of unauthorized software programs" using McAfee Application Control and will work towards building and implementing a whitelist.

Remaining project activities are scheduled to be completed by the end of January 2018 to implement a VA Blacklist with McAfee Application Control. Linux testing of McAfee Application Control is underway. After testing is completed, the blacklist is expected to be implemented on Linux machines by the end of January 2018. Once the Blacklist has been implemented VA project teams will begin developing the Whitelist, estimated fully implemented VA Whitelist by FY2019.

Accomplishments for this Recommendation:

- Began implementation of a Blacklist of software not approved for use on VA networks. The project is scheduled to be completed by the end of January 2018
- Developed a process to update the TRM site, which presents a list of assessed technologies and standards used to develop, operate, and maintain enterprise applications
- Implemented BDNA normalization monitoring tool within the VA environment
- Developed a training and communications plan for monitoring, preventing installation, and removing of unauthorized software
- Developed a SOP for unapproved, prohibited, and unmanaged software remediation
- Developing monthly configuration management vulnerabilities remediation reports
- Entering enterprise software titles into the TRM portal on a monthly basis
- Submitting updates to the TRM portal on a monthly basis with enterprise software titles, which were previously not entered into the TRM portal
- Developing remediation reports for newly identified unapproved, prohibited, and unmanaged software across the enterprise on a monthly basis
- Removing identified unapproved, prohibited and unmanaged software across the enterprise on a monthly basis

Target Completion Date: In progress

Recommendation 25: We recommended the Executive in Charge for Information and technology develop a comprehensive software inventory process to identify major and minor software applications used to support VA programs and operations. (This is a repeat recommendation from prior years.)

OI&T Response: VA Concurs. Within VA, hardware assets have been defined in a formal process, which is consistently implemented throughout the enterprise. Equipment items are entered into an Automated Information System (AIS) for accountability and tracking purposes, as outlined is VA Directive and Handbook 7002. VA's current system is referred to as Automated Engineering Management / Medical Equipment Reporting System (AEMS/MERS). In 2016 a decision was made by VHA to migrate off AEMS/MERS to IBM's Maximo Commercial Off the Shelf (COTS) application. The project was implemented under the Service Oriented Architecture Research and Development (SOARD) Program Management Office. VA migrated 38 sites to Maximo and are no longer using AEMS/MERS. Both systems, along with the data, is maintained by VHA Logistics. The remaining 97 disparate databases, in addition to the Maximo data, are consolidated on a weekly basis to the Corporate Data Warehouse, allowing for a holistic view of IT equipment items. Items cataloged in the AIS should consider be inventoried annually to a space. This requires that IT staff visit each asset and scans the asset barcode to the space label of the room. Of the 1.81 million assets in the AIS, OI&T has maintained an annual inventory compliance of 96%, meaning that 96% (1.73 million assets) have an annual inventory date of less than 1 year. Work is underway to allow for the use of online tools to constitute an

inventory event. As of 10/18/2017, VA has a total of 560,000 items cataloged in Maximo, while 1.25M assets are cataloged in AEMS/MERS.

VA is modernizing the hardware asset inventory system by replacing it with a Government off the Shelf (GOTS) or Commercial off the shelf (COTS) software solution. This solution will transition VA from numerous disparate systems and databases to a single database operating under a modern industry standard platform. Requirements include the ability to upload asset information, rather than using logisticians to enter serial numbers and other asset attributes into the AIS. In addition, the solution is expected to allow for user-level assignment of mobile assets and automated renewal of annual inventory. Furthermore, OI&T began linking the AIS to online tools in order to reduce the need for an annual physical inventory of each asset.

For documenting and monitoring inventory of installed software across the enterprise, VA currently uses the Technical Reference Model (TRM) site to present a list of assessed software technologies and standards used to develop, operate, and maintain enterprise applications. VA utilizes available tools (e.g., BDNA, System Center Configuration Manager (SCCM), TRM, Security Management and Analytics (SMA) Vulnerability reports) to analyze and inventory installed software across the enterprise. In the event that software is not classified within TRM, the software considered "unmanaged". A team of analysts work through the unmanaged software identified on the network, and submits to TRM for review and classification as part of the unauthorized software management process. Once a TRM determination is made the team assists in remediation/removal of software identified as unauthorized.

Accomplishments for this Recommendation:

- Began implementation of a Blacklist of software not approved for use on VA networks. The project is scheduled to be completed by the end of January 2018
- Developed a process to update the TRM site, which presents a list of assessed technologies and standards used to develop, operate, and maintain enterprise applications
- Implemented BDNA normalization monitoring tool within the VA environment
- Developed a training and communications plan for monitoring, preventing installation, and removing of unauthorized software
- Developed a SOP for unapproved, prohibited, and unmanaged software remediation
- Developing monthly configuration management vulnerabilities remediation reports
- Entering enterprise software titles into the TRM portal on a monthly basis
- Submitting updates to the TRM portal on a monthly basis with enterprise software titles, which were previously not entered into the TRM portal
- Developing remediation reports for newly identified unapproved, prohibited, and unmanaged software across the enterprise on a monthly basis
- Removing identified unapproved, prohibited and unmanaged software across the enterprise on a monthly basis

Migrated 38 sites to Maximo and are no longer using AEMS/MERS. **Target Completion Date**: In progress

Recommendation 26: We recommended the Executive in Charge 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 initial audit findings, the assessed contractor-managed cloud based systems addressed the discovered vulnerabilities within the VA's time frame. Any item which cannot be remediated with the time frame has a documented POAM. These are updated monthly within the VA's GRC tool (Risk Vision) to ensure complete transparency and compliance.

In addition to remediating the specific findings, The Department of Veterans Affairs (VA) is establishing a VA Enterprise Cloud (VAEC) as a business enabler that will efficiently provide Veterans, their dependents, VA employees and contractors, and VA partners with innovative, Veteran-focused services, applications, and access to information on demand using Veteran-preferred devices and technologies. The VAEC will become the foundation of an agile, interoperable, scalable, and secure cloud computing environment that can adapt to evolving business needs. It will offer elastic, metered data storage and computing capability to support new approaches for the delivery of integrated services to Veterans. The benefits of an enterprise cloud infrastructure and platform services, characterized by costs shared across a broad customer base and supported by leading, external technology providers, will improve the VA's ability to target its efforts toward key mission areas focused on the Veteran. This will result in more efficient and responsible stewardship of taxpayer dollars. The VAEC is intended to improve security of all VA Cloud efforts by leveraging FedRAMP and FISMA Guidelines and standardizing cloud hosting environments.

The VAEC is a multi-vendor platform for the development and deployment of VA cloud applications that can host applications at all FedRAMP security levels – High, Moderate and Low. The VAEC provides a set of common, general support services (GSS) such as authentication and performance monitoring which each application can leverage, speeding and simplifying the development of new applications in or migration of existing applications to the VAEC. The VAEC inherits security controls from the underlying FedRAMP Authorized CSP, it implements many of the NIST-, FedRAMP- and VA-required security controls for inheritance by applications hosted in the VAEC in order to standardize security and reduce the time each application should take to obtain a VA [Authority to Operate] (ATO). It also provides for isolated and standardized security scanning, security logging, monitoring, and security reporting capabilities for use by all applications hosted within the VAEC.

Initially, the VAEC will include the two leading commercial cloud platforms: Amazon Web Services (AWS) GovCloud and Microsoft Azure Government (MAG). Both have met stringent federal security requirements including a FedRAMP High authorization and received a VA ATO. The VAEC will also include an on-site, VA Private Cloud, for applications with data sensitivity, technical architecture or performance requirements that require them to be hosted in an on-premises cloud. The VA is in the process of acquiring an Enterprise Cloud Management Platform (CMP) and Cloud Access Security Broker (CASB) tools later this year to enhance management and security capabilities of the VAEC. By early FY2019, the VAEC will add an on premises private cloud and be integrated with VA's recently acquired ServiceNow ITSM CMDB solution for improved configuration management of cloud resources. For applications that do not fully leverage VAEC cloud computing services process comprehensive processes are being put in place to continue to provide consistent support across the Department.

By migrating existing applications to and developing new applications in the VAEC the VA will be able to address and remediate the findings in this recent OIG report. In addition the VAEC is intended to support the OIS efforts to improve VA Cloud Security. In 2017, OIS appointed an Enterprise Cloud Security Architect to develop security policies, processes, and standards around cloud at VA. In FY17, the Cloud Security Architecture team developed a cloud security framework and requirements that map

to the CSF and a VA Cloud Overlay that includes the FedRAMP Control Baseline. Recently, the Enterprise Cloud Security Architect awarded two security support services contracts for cloud architecture and engineering security support (4th Qtr. FY17 and early FY18). These teams have developed draft VA Cloud Security Guidelines, Cloud Security Strategy, and an Integrated System Security Standard Operating Procedural document for System Owners, Program Managers, Information Security Officers, and other stakeholders with the intention to modernize, streamline, and introduce security protection efficiency across the Department. These teams will continue to build relationships/partnerships across the VA and its Administrations, providing security support to the application migration process, creating additional cloud overlays and baselines, cloud application continuous monitoring support, performing security testing of cloud applications, and designing processes that will further secure VA cloud environments and applications. **Target Completion Date:** In Progress

Recommendation 27: We recommended the Executive in Charge for Information and technology implement 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. VA uses the Technical Reference Model (TRM) site to present a list of assessed technologies and standards used to develop, operate, and maintain enterprise applications. Software not classified within TRM is considered "unmanaged". A team of analysts works through the backlog of unmanaged software currently installed on the network, utilizing available tools (e.g., BDNA, System Center Configuration Manager (SCCM), TRM, Google, Security Management and Analytics (SMA) Vulnerability reports) to prioritize and analyze these titles and submit to TRM for review and classification. Additionally, the team surveys VA's network of end-users to determine the business need for software technologies prior to submission to TRM.

While VA does not have a fully developed and implemented software "Whitelist" of approved software for use on the VA network, VA does have an active and funded project to develop and implement a Blacklist of software that is not approved for use on the VA network. The Blacklist project focuses on the deployment of the Continuous Diagnostics and Mitigation (CDM) Software Asset Management (SWAM) capability and is part of a larger CDM deployment effort in collaboration with the Department of Homeland Security (DHS). Following NIST guidelines, VA will "prevent the execution of unauthorized software programs" using McAfee Application Control and will work towards building and implementing a whitelist.

Remaining project activities are scheduled to be completed by the end of January 2018 to implement a VA Blacklist with McAfee Application Control. Linux testing of McAfee Application Control is underway. After testing is completed, the blacklist is expected to be implemented on Linux machines by the end of January 2018. Once the Blacklist has been implemented VA project teams will begin developing the Whitelist, estimated fully implemented VA Whitelist by FY2019.

Accomplishments for this Recommendation:

- Began implementation of a Blacklist of software not approved for use on VA networks. The project is scheduled to be completed by the end of January 2018
- Developed a process to update the TRM site, which presents a list of assessed technologies and standards used to develop, operate, and maintain enterprise applications

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

Removing identified unapproved, prohibited and unmanaged software across the enterprise on a monthly basis. **Target Completion Date:** In progress

Recommendation FY 2006-04: We recommended the Executive in Charge 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. The Office of Operations, Security and Preparedness (OSP) has formed the Access and Identity Management (AIM) Program Management Office (PMO), formerly the Identity, Credential, and Access Management (ICAM) PMO. The AIM mission is to establish an enterprise-wide standardized, and integrated, process for onboarding, monitoring, and off-boarding VA Employees, Contractors, Health Care Professional Trainees, and Affiliates through an automated solution, known as the VA Onboarding Solution. Several critical components of the VA Onboarding Solution will be the integration with HR-Smart (an authoritative Human Resource Information System [HRIS] the replacement to PAID), USA Staffing, and the establishment of an authoritative source for Contractor identity data via the IAM Identity Services System. These authoritative sources will allow the VA Onboarding Solution to establish unique digital identities for Employees and Contractors, allowing for a shift from manual to automated processes used to monitor when employees and contractors change positions, change access requirements (elevated access) and when they leave VA. Future versions of the system will provide a portal to enter Volunteers and Affiliates information directly into the centralized VA Onboarding Solution.

OSP, Personnel Security & Credential Management (PSCM), formerly the Personnel Security & Suitability (PSS) PMO, has procured a Commercial Off-The Shelf (COTS) product to serve as a VA-wide personnel security and suitability case management system. The system, VA Centralized Adjudication and Background Investigation System (VA-CABS), will integrate with the VA Onboarding Solution. VA-CABS, will establish business rules based on the position description and the risk and sensitivity levels of the position to ensure investigations are initiated at the required level within the permitted timelines. VA CABS will also track reinvestigation timelines to initiate re- investigations at the designated time. This will decrease the number of individuals with outdated investigations. The VA-CABS contract was awarded in August 2017, and is scheduled to be in a production environment in July 2018.

Accomplishments for this Recommendation:

- Selected an enterprise wide COTS case management system for maintaining background investigation and adjudication data
- Implemented improved processes to allow local facilities track and initiate reinvestigations for employees in high-risk positions in a timely manner to align with the intent of the POA.
- Completed Policy advisory PSIM 15-02 which addresses the following task: Contracting Officer's Representative (COR) to monitor contract status and track their contractor's investigation status
- Developed training and communication processes and requirements to assist with tracking and facility functions
- Updated VA Handbook 0710, Personnel Security and Suitability Program, to provide policy updates to the field For VA Onboarding Solution:
- Completed Enterprise Acquisition Systems (EAS) Service Bus (Electronic Contract Management System (eCMS)) integration with the VA Onboarding Solution (formerly known as ICAM Onboarding Solution)
- Completed the HR-Smart Solution integration and deployment towards the overall VA Onboarding Solution
- Completed the Talent Management System (TMS) integration and deployment towards the overall VA Onboarding Solution

Completed User Interface and workflows for Contractor onboarding/off-boarding using VA Onboarding Solution. **Target Completion Date**: In progress

Recommendation FY 2006-09: We recommended the Executive in Charge for Information and technology identify and deploy solutions to encrypt sensitive data and resolve clear text protocol vulnerabilities.

OI&T Response: VA does not concur with this recommendation due to the project being completed as of March 2017. OIT could find no references to clear text protocol findings in any of the FY17 reports. 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.

Target Completion Date: VA closed this finding in March 2017.

OIG Response: We have reviewed VA's corrective action plan and supporting documentation and consider this recommendation closed.

APPENDIX E: 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 the OIG website at www.va.gov/oig/.