DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

DEPARTMENT OF VETERANS AFFAIRS

Federal Information Security Modernization Act Audit for Fiscal Year 2018

AUDIT	REPORT # 18-02127-64	MARCH 12, 2019

The mission of the Office of Inspector General is to serve veterans and the public by conducting effective oversight of the programs and operations of the Department of Veterans Affairs through independent audits, inspections, reviews, and investigations.

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 2018

To: Assistant Secretary for Information and Technology

1. Enclosed is the final audit report, *Federal Information Security Modernization Act Audit for Fiscal Year 2018*. The Office of Inspector General (OIG) contracted with the independent public accounting firm, CliftonLarsonAllen LLP, to assess the Department of Veterans Affairs’ (VA) information security program in accordance with the Federal Information Security Modernization Act (FISMA).

2. To ensure the adequacy and effectiveness of information security controls, FISMA requires agency program officials, Chief Information Officers, and Inspectors General to conduct annual reviews of agencies’ information security 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. Accordingly, the OIG does not express an opinion on VA’s information security program in place during fiscal year (FY) 2018. The OIG’s independent auditors will follow up on the outstanding recommendations and evaluate the adequacy of corrective actions during their FY 2019 FISMA audit.

4. According to findings by CliftonLarsonAllen LLP, 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 2018 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.
    - 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 28 recommendations for improving VA’s information security program. Twenty-seven recommendations are included in the report body and one recommendation is provided in Appendix A. The recommendation in Appendix A addresses the status of a prior year recommendation and VA’s plans for corrective action. VA successfully closed one recommendation in FY 2018. Specifically, the OIG closed recommendation FY 2006-09 from a prior year as VA deployed solutions to encrypt sensitive data and resolve clear text protocol vulnerabilities.

6. The Principal Deputy Assistant Secretary for Information and Technology concurred with 25 of 28 recommendations and provided acceptable action plans in response to these recommendations. While the Principal Deputy Assistant Secretary did not concur with three recommendations, the OIG believes these recommendations warrant further attention from VA and will follow up on these issues during the FY 2019 assessment. Further details on OIT’s nonconcurrence, and the OIG’s response, are provided on pages 5 and 13 of this report.

7. The effect of the open recommendations will be considered in the FY 2019 assessment of VA’s information security posture. The OIG remains concerned that continuing delays in implementing effective corrective actions to address these open recommendations could potentially contribute to reporting an information technology material weakness for the FY 2019 audit of VA’s Consolidated Financial Statements.

Larry M. Reinkemeyer

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

Abbreviations

CLA	CliftonLarsonAllen LLP
DHS	Department of Homeland Security
ECSP	Enterprise Cybersecurity Strategy Program
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GRC	Governance Risk and Compliance
NIST	National Institute of Standards and Technology
OIT	Office of Information and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plans of Action and Milestones
SCA	Security Controls Assessment
VA	Department of Veterans Affairs

CliftonLarsonAllen

CliftonLarsonAllen LLP
CLAconnect.com

February 21, 2019

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

Dear Mr. Missal:

CliftonLarsonAllen LLP (CLA) conducted a performance audit of the United States Department of Veterans Affairs' (VA) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) for the fiscal year ended September 30, 2018. The objective of this audit was to determine the extent to which VA's information security program and practices comply with 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) information security guidelines. The audit included the testing of selected management, technical, and operational controls outlined in NIST's Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

Our audit was performed in accordance with the performance audit standards specified in *Government Auditing Standards*, issued by the Comptroller General of the United States. 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 based on our audit objectives.

Our procedures were designed to respond to the FISMA-related questions outlined in the OMB template for the Inspectors General and evaluate the VA information security program's compliance with FISMA and applicable NIST information security guidelines, as defined in our audit program. The audit included the evaluation of 49 selected major applications and general support systems hosted at 25 VA facilities that support the National Cemetery Administration, the Veterans Benefits Administration, and the Veterans Health Administration lines of business. Audit fieldwork occurred during the period April 2018 through November 2018.

Based on our audit procedures, we conclude that VA continues to face significant challenges meeting the requirements of FISMA. This report provides 28 recommendations to assist VA in strengthening its information security program.

In connection with the audit of VA's FY 2018 Consolidated Financial Statements, CLA evaluated general computer and application controls for VA's major financial management systems. Significant deficiencies identified during CLA's evaluation are included in this report. In addition to the findings and recommendations in the accompanying report, our conclusions related to VA's information security program are contained within the OMB FISMA reporting template provided to the OIG in October 2018.

This report is intended solely for the information and use of the management of the VA, the VA OIG and the Government Accountability Office and not intended to be and should not be used by anyone other than these specified parties.

Sincerely,

CliftonLarsonAllen LLP

CliftonLarsonAllen LLP
Arlington, Virginia

Contents

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 (CLA) to perform the FY 2018 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 49 major applications and general support systems at 25 VA facilities. In FY 2018, 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 28 recommendations for improving VA's information security program: 27 recommendations are included in the report body and one recommendation is 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 2018 FISMA audit. VA successfully closed one recommendation in FY 2018. The FY 2017 FISMA report provided 29 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 2018, the VA's Acting Chief Information Officer continued the Enterprise Cybersecurity Strategy Program (ECSP) 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 ECSP 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 ECSP team has launched 31 Plans of Action to address previously identified security weaknesses and the IT material weakness. As part of the ongoing ECSP efforts, we noted continued improvements related to:

- Improved security documentation
- Centralization of control functions
- Further maturation of predictive scanning process
- 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. Additionally, controls need to be applied in a holistic manner to information systems across VA in order to be considered consistent and fully effective. 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 action and milestones, and security control assessments (SCAs). 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 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 previously known or identified system security risks. Specifically, we identified SCAs where valid weaknesses were not incorporated into overall risk management activities. We also identified issues related to the incomplete reporting of control deficiencies identified during SCAs and noted that four systems were granted Authority to Operate without undergoing a timely 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 11,734 open POA&Ms in FY 2018, as compared with 8,500 open POA&Ms in FY 2017. The increase can be attributed to a change in the way security control assessment results were handled during the year. For instance, in the beginning of the year, control assessment results were screened before entry as POA&Ms; however, by the end of the year, VA was making POA&Ms for all control assessment results, which contributed to the overall increase. 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 what actions must be taken to remediate system security risks and improve VA's overall information security posture.

VA has made progress in managing 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&Ms that were not updated to accurately reflect their current status, (c) POA&Ms were not consistently updated to consider all known security weaknesses, and (d) security deficiencies for several unrelated controls that were consolidated under one POA&M instead of tracking them separately.

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, control status, and control implementation details that were not supported by evidence. 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.

A. CORRECTIVE ACTIONS RECOMMENDED

1. We recommended the Executive in Charge for Information and Technology consistently implement the agency-wide risk management governance structure, along with mechanisms to identify, monitor, and manage risks across the enterprise. *(This is a modified 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 Action 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 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 security

plans 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.)*

Management Comments

The Principal Deputy Assistant Secretary for Information and Technology did not concur with Recommendation 1 but concurred with Recommendations 2, 3, 4, 5, and 6. For Recommendation 1, the Principal Deputy Assistant Secretary non-concurred and stated that VA has aligned its risk management framework to provide visibility into cybersecurity risk and ultimately make risk-based determinations for an information system's Authority to Operate. To address Recommendation 2, VA is tracking the implementation of the new GRC solution, as a project within the Enterprise Cybersecurity Strategy Program that will support remediation of weaknesses identified around the authorization lifecycle. For Recommendation 3, VA is expanding its POA&M efforts to accurately document remediation efforts prior to closure through its GRC tool. In response to Recommendation 4, VA is expanding its POA&M process to consistently detect, evaluate, and monitor the current state of identified security weaknesses. To address Recommendation 5, VA's Case Management process will provide a systematic approach for continuous evaluation of system security plans for identification of security controls as they apply to the current operational environment. For Recommendation 6, VA is modifying its procedures for tracking deficient security controls that will provide a detailed view that highlights which security risks have been fully mitigated and which still require remediation.

OIG Response

The Principal Deputy Assistant Secretary's planned corrective actions are responsive to Recommendations 2, 3, 4, 5, and 6. Regarding VA's non-concurrence to Recommendation 1, within the report we stated that 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. Specifically, risk assessments did not always consider all previously known or identified system security risks. Additionally, we identified security control assessments where valid weaknesses were not incorporated into overall risk management activities. Accordingly, we stand by our original finding and recommendation. The OIG will monitor VA's progress and follow up on implementation of the recommendations until all proposed actions are completed. Appendix D provides the full text of the Principal Deputy Assistant Secretary's comments.

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. The 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

Reviews of systems and permission settings 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, 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 always enabled, effectively managed, aggregated, or proactively reviewed for certain significant systems, such as Veterans Health Information Systems and Technology Architecture, and users with excessive privileges given their job responsibilities. 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 the 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 FY 2018. 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.

B. 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 to the extent feasible for all user accounts throughout the agency. *(This is a modified repeat recommendation from prior years.)*

Management Comments

The Principal Deputy Assistant Secretary for Information and Technology concurred with Recommendations 7, 8, 9, and 10. For Recommendation 7, the Principal Deputy Assistant Secretary stated that VA is currently taking measures to address the findings regarding service account password configuration and the service account password change process, based on the deployment of a technological solution. To address Recommendation 8, VA is working with the Department of Homeland Security to create a master user record. This record will pull-in data from multiple sources to build an access record for users at the VA network. In addition, VA is working on developing policy for financial applications, outlining annual user account reviews for adding, modifying, and/or deleting user accounts. In response to Recommendation 9, VA will continue to improve system owner accountability and communication with the Cyber Security Operations Center to ensure that audit logging for critical systems is performed. For Recommendation 10, VA is taking necessary mitigations to reduce the risk to the enterprise by implementing compensating controls.

OIG Response

The Principal Deputy Assistant Secretary's planned corrective actions are responsive to Recommendations 7, 8, 9, and 10. The OIG will monitor VA's progress and follow up on implementation of the recommendations until all proposed actions are completed. Appendix D provides the full text of the Principal Deputy Assistant Secretary's comments.

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 our 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 into VA information systems. NIST SP 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

While VA has made improvements in correcting database vulnerabilities, our database assessments continue to identify a number of unsecure configuration settings that could allow any database user to gain excessive unauthorized access permissions to critical system information. NIST SP 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.

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 SP 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 the trusted hosts that connect to them 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 trusted hosts that were connected to VA's general network. These insecure hosts were given the ability to access medical devices behind the Medical Device Isolation Architecture.

Although there were improvements in identification of vulnerabilities, VA did not perform comprehensive and credentialed vulnerability scans of all 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, OIT 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) insecure database configuration privileges, and (3) an unsecured file directory which included potential sensitive patient information.

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 OIT 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 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.

C. 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 configuration for all platforms and ensure all baselines are appropriately implemented for compliance with established VA security standards. *(This is a repeat recommendation from prior years.)*
14. We recommended the Executive in Charge for Information and Technology implement improved network access controls to restrict medical devices from the general network and ensure that databases, file shares, and management devices, are adequately secured prior to connecting to VA’s network. *(This is a modified 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.)*

Management Comments

The Principal Deputy Assistant Secretary for Information and Technology concurred with Recommendations 11, 12, 13, 14, 15, and 16. For Recommendation 11, the Principal Deputy Assistant Secretary stated that VA commissioned the establishment of a centralized vulnerability management program office in FY 2018 to strengthen processes related to the identification, classification, remediation, and mitigation of vulnerabilities throughout the enterprise. To address Recommendation 12, VA Security Management has initiated projects to address gaps in vulnerability scanning and credential management and to strengthen and standardize patch and vulnerability management practices across the enterprise. In response to Recommendation 13, VA is in the process of developing and implementing enhanced processes for security baseline creation, implementation, testing, and monitoring. For Recommendation 14, VA has implemented and enterprise-wide system vulnerability management program and reported a strategy for segregating medical devices to better protect sensitive information is in the process of being implemented. In response to Recommendation 15, VA reported they have implemented a continuous monitoring process to ensure the integrity and compliance of “access control lists” to ensure the continued provision of direct treatment, diagnostics, and monitoring of patient care by VA’s medical devices. To address Recommendation 16, VA has commissioned the establishment of a centralized vulnerability management program office in FY 2018 to strengthen processes related to the identification, classification, remediation, and mitigation of vulnerabilities throughout the enterprise.

OIG Response

The Principal Deputy Assistant Secretary’s planned corrective actions are responsive to Recommendations 11, 12, 13, 14, 15, and 16. The OIG will monitor VA’s progress and follow up on implementation of the recommendations until all proposed actions are completed. Appendix D provides the full text of the Principal Deputy Assistant Secretary’s comments.

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.

Change management policies and procedures for authorizing, testing, and approving system changes were not consistently implemented for mission-critical applications and networks. We identified numerous test plans, test results, risk and impact analyses, and approvals that were either incomplete or missing for certain General Support Systems and major applications. 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.

D. CORRECTIVE ACTION 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.)*

Management Comments

The Principal Deputy Assistant Secretary for Information and Technology concurred with Recommendation 17. For Recommendation 17, the Principal Deputy Assistant Secretary stated that VA is developing and implementing an enterprise-wide system to facilitate consistent change management of financial applications and networks.

OIG Response

The Principal Deputy Assistant Secretary's planned corrective actions are responsive to Recommendation 17. The OIG will monitor VA's progress and follow up on implementation of the recommendation until all proposed actions are completed. Appendix D provides the full text of the Principal Deputy Assistant Secretary's comments.

5. Contingency Planning

VA contingency plans were not consistently and comprehensively reviewed as unplanned outages and disruptions occurred. While we noted some improvements to secure backup data, VA backup 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 one mission-critical system were not encrypted prior to transporting data offsite for storage.
- There were instances of unplanned outages or disruptions where services were not recovered within prescribed Recovery Time Objectives. Furthermore, these instances did not prompt Contingency Plan reviews or updates in accordance with defined policy. Without reviewing and updating contingency plans as issues are encountered, the VA is at risk of not being able to adequately respond to and recover from outage events or disasters.

E. CORRECTIVE ACTIONS RECOMMENDED

18. We recommended the Executive in Charge for Information and Technology implement improved processes for ensuring that backup data is adequately secured in accordance with organizational policy*. (This is a repeat recommendation from prior years.)*
19. We recommended the Executive in Charge for Information and Technology implement improved processes for the review of system outages and disruptions for contingency plan improvements in accordance with defined policy. *(This is a modified repeat recommendation from prior years.)*

Management Comments

The Principal Deputy Assistant Secretary for Information and Technology did not concur with Recommendations 18 and 19. Regarding Recommendation 18, the Principal Deputy Assistant Secretary stated that VA has implemented measures to safely secure, store, and restore certain legacy backup tapes. For Recommendation 19, the Principal Deputy Assistant Secretary stated that the network and system outages identified by OIG were deemed as minor disruptions that would not warrant the initiation of IT Contingency / Disaster Recovery Plans.

OIG Response

Regarding VA’s non-concurrence to Recommendation 18, within the report we identified certain legacy backup tapes for mission critical systems were not encrypted prior to transporting data offsite for storage. While VA has indicated that all legacy tapes have since been securely stored and will no longer be transported offsite until they are decommissioned, this effort was not completed until the later parts of the year and could not be fully tested. Accordingly, we stand by our original finding and recommendation. Regarding VA’s non-concurrence to Recommendation 19, within the report we identified instances of unplanned system outages that were not recovered within prescribed Recovery Time Objectives and these events did not prompt Contingency Plan reviews or updates in accordance with defined policy. Although VA indicated that the events were minor, adequate documentation was not provided to support their statement. Furthermore, we noted that most of the system outages took place on Regional General Support System components that are rated as “high” impact based on VA’s FISMA system categorizations. Therefore, we stand by our original finding and recommendation. The OIG will monitor VA’s progress and follow up on implementation of the recommendations until all proposed actions are completed. Appendix D provides the full text of the Principal Deputy Assistant Secretary’s comments.

6. Incident Response and Monitoring

Although progress has been made in relation to incident response metrics and network protections, deficiencies were noted in several areas including security event monitoring, security event correlation, host based protections and monitoring, vulnerability scan monitoring, and incident reporting.

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 had seven 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 Cybersecurity 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 two major data centers, ten VA medical centers, two Regional Offices, the Health Resource Center, and the Financial Services Center. The process for tracking, updating, and reporting security-related incidents was not performed consistently throughout the year.

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 Cybersecurity Operations Center did not have full visibility to evaluate all security-related audit data throughout the enterprise for the entire year. Management plans to increase centralized visibility to more platforms moving forward to support the 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 three unannounced scans of internal networks, and despite Federal requirements for detecting this type of activity, none of these scans were blocked by the Cybersecurity 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.

C. Incident Response Tracking and Reporting

Throughout the year, we identified several instances of security events that were not reported as incident tickets within the timeframes required by VA Handbook 6500. Additionally, we identified several instances of open tickets that were not reviewed or updated in a timely manner in accordance with documented policy.

D. 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 Cybersecurity 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 on VA networks. (*This is a modified repeat recommendation from prior years.*)

Management Comments

The Principal Deputy Assistant Secretary for Information and Technology concurred with Recommendations 20, 21, 22, and 23. For Recommendation 20, the Principal Deputy Assistant Secretary stated that VA is in the process of developing and implementing an enterprise-wide workflow to centralize the oversight and authorizing of interconnection agreements to determine completeness and quality. In response to Recommendation 21, VA continues to develop new processes and tracking of metrics to strengthen the agency-wide incident response process. For Recommendation 22, VA is working toward integrating technological solutions that will allow for improved visibility and monitoring, investigations, and adversarial hunting across the enterprise. To address Recommendation 23, VA's Cybersecurity Management is in the process of initiating a project to leverage the enterprise ForeScout Infrastructure Threat Protection capabilities to identify unauthorized scanning across the enterprise.

OIG Response

The Principal Deputy Assistant Secretary's planned corrective actions are responsive to Recommendations 20, 21, 22, and 23. The OIG will monitor VA's progress and follow up on implementation of the recommendations until all proposed actions are completed. Appendix D provides the full text of the Principal Deputy Assistant Secretary's comments.

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 system inventory to identify applications and components that support critical programs and operations. NIST SP 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, we noted that certain system security deficiencies were not incorporated into POA&M management and risk management activities. Additionally, security deficiencies and weaknesses for several controls were improperly consolidated into one control weakness. This process did not effectively communicate or track the breadth and depth of the risk affecting the environment.

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. System 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 logical and physical components supporting critical programs and operations. Incomplete inventories of critical components could hinder VA’s patch and vulnerability 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.

E. 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 prohibited software on agency devices. *(This is a modified repeat recommendation from prior years.)*

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

Management Comments

The Principal Deputy Assistant Secretary for Information and Technology concurred with Recommendations 24 and 25. For Recommendation 24, the Principal Deputy Assistant Secretary stated that VA is in the process of evaluating enterprise tools to identify and prevent the use of unauthorized software on agency devices. To address Recommendation 25, VA is in the process of developing enhanced processes to accurately inventory software and hardware across the enterprise.

OIG Response

The Principal Deputy Assistant Secretary’s planned corrective actions are responsive to Recommendations 24 and 25. The OIG will monitor VA’s progress and follow up on implementation of the recommendations until all proposed actions are completed. Appendix D provides the full text of the Principal Deputy Assistant Secretary’s comments.

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.

- We identified significant control weaknesses on contractor managed systems such as HR Smart and the VA Loan Electronic Reporting Interface.
- 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.

F. CORRECTIVE ACTIONS RECOMMENDED

26. We recommended the Executive in Charge for Information and Technology implement improved procedures for overseeing contractor-managed systems and ensure information security controls adequately protect VA sensitive systems and data. *(This is a modified repeat recommendation from prior years.)*
27. We recommended the Executive in Charge for Information and Technology implement mechanisms for updating their 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.)*

Management Comments

The Principal Deputy Assistant Secretary for Information and Technology concurred with Recommendations 26 and 27. For Recommendation 26, the Principal Deputy Assistant Secretary stated that VA monitors contractor-hosting facilities' connections, which fulfills continuous monitoring requirements for VA systems hosted outside the VA network. This connections monitoring is expected to be expanded to new remote Business Partners. To address Recommendation 27, VA is in the process of improving mechanisms for system inventory management across the enterprise.

OIG Response

The Principal Deputy Assistant Secretary’s planned corrective actions are responsive to Recommendations 26 and 27. The OIG will monitor VA’s progress and follow up on implementation of the recommendations until all proposed actions are completed. Appendix D provides the full text of the Principal Deputy Assistant Secretary’s comments.

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, one recommendation remains 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 A.1. 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.

Management Comments

The Principal Deputy Assistant Secretary for Information and Technology concurred with Recommendation FY 2006-04. To address this Recommendation, the Principal Deputy Assistant Secretary stated that VA is in the process of developing and implementing an enterprise-wide onboarding, monitoring, and off-boarding solution referred to as the VA Onboarding Solution.

OIG Response

The Principal Deputy Assistant Secretary's planned corrective actions are responsive to Recommendation FY 2006-04. The OIG will monitor VA's progress and follow up on implementation of the recommendations until all proposed actions are completed. Appendix D provides the full text of the Principal Deputy Assistant Secretary's comments.

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 October 2017, OMB issued Memorandum M-18-02, *Fiscal Year 2017-2018 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 2018 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, data protection and privacy, incident response, risk management, security training, and contingency planning. The OIG contracted with the independent accounting firm CliftonLarsonAllen LLP to conduct the annual FISMA audit for FY 2018. 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 49 selected major applications and general support systems hosted at 25 VA facilities that support the National Cemetery Administration, the Veterans Benefits Administration, and the Veterans Health Administration lines of business. We performed vulnerability assessments and evaluated management, operational, technical, and application controls supporting major applications and general support systems.

In connection with the audit of VA's FY 2018 Consolidated Financial Statements, CLA 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 CLA'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:

- Information Technology Center—Austin, TX
- VA Financial Services Center—Austin, TX
- VA Medical Facility—Baltimore, MD
- VA Medical Facility—Bay Pines, FL
- VA Medical Facility—Clarksburg, WV
- Verizon, Cloud Service Provider—Culpeper, VA
- VA Medical Facility—Dallas, TX
- VA Medical Facility—Fayetteville, AR
- Information Technology Center—Hines, IL
- VA Medical Facility—Los Angeles, CA
- VA Regional Office—Los Angeles, CA
- Network Security Operations Center—Martinsburg, WV
- Capital Region Readiness Center—Martinsburg, WV

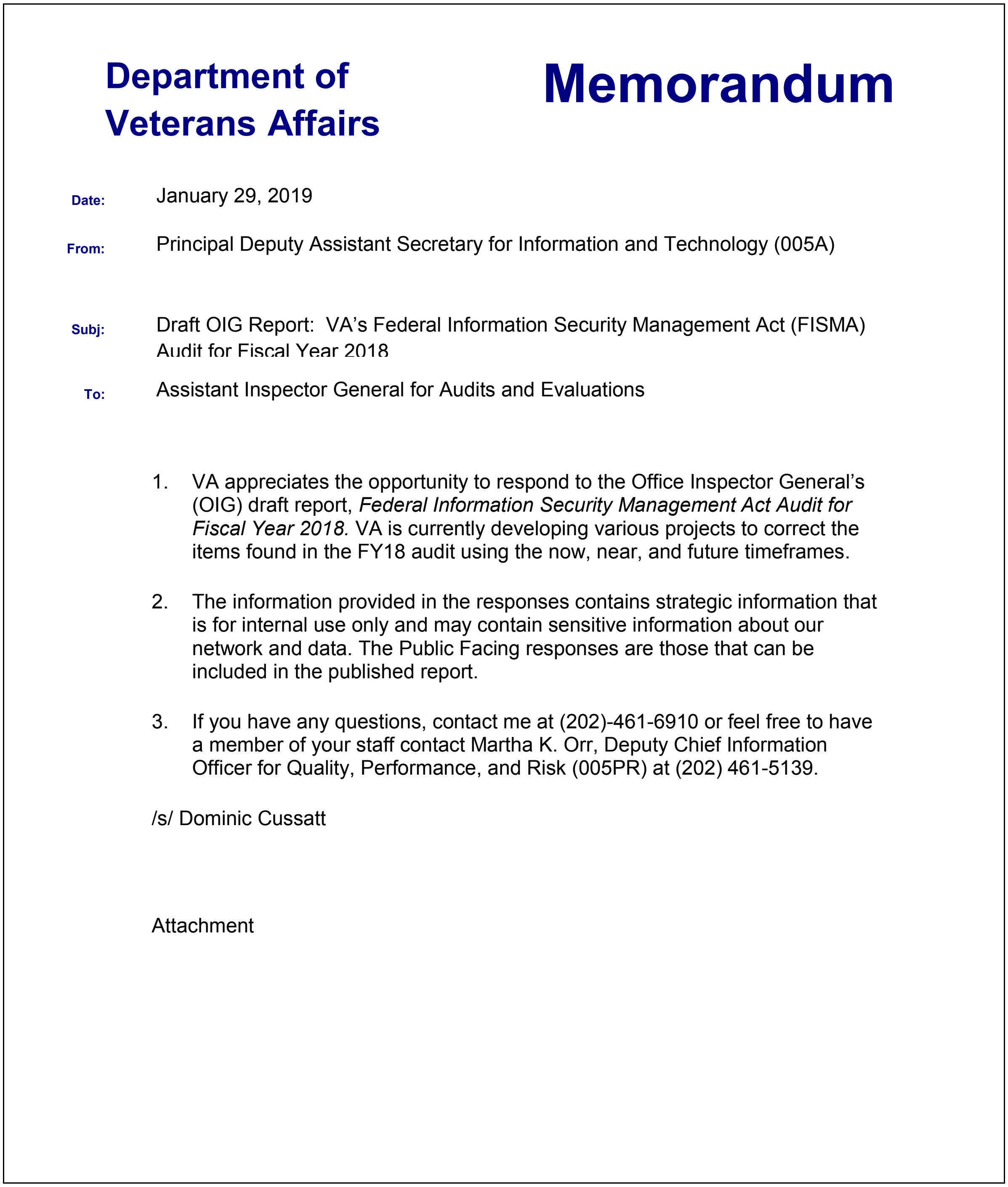
- VA Medical Facility—Mountain Home, TN
- VA Medical Facility— Muskogee, OK
- VA Regional Office—Muskogee, OK
- Information Technology Center—Philadelphia, PA
- National Cemetery Administration—Quantico, VA
- VA Medical Facility—Seattle, WA
- VA Regional Office—St. Petersburg, FL
- Loan Guaranty Contractor Managed Facility—Tampa, FL
- VA Medical Facility—Togus, ME
- Health Resource Center—Topeka, KS
- VA Medical Facility—Tucson, AZ
- VA Central Office—Washington, DC

During site visits, we evaluated 49 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

CLA conducted this audit in accordance with performance auditing standards, as specified in the Government Accountability Office's *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.

Appendix D: Principal Deputy Assistant Secretary for Information and Technology Comments



Department of Veterans Affairs

Memorandum

Date: January 29, 2019

From: Principal Deputy Assistant Secretary for Information and Technology (005A)

Subj: Draft OIG Report: VA's Federal Information Security Management Act (FISMA) Audit for Fiscal Year 2018

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 2018.* VA is currently developing various projects to correct the items found in the FY18 audit using the now, near, and future timeframes.

2. The information provided in the responses contains strategic information that is for internal use only and may contain sensitive information about our network and data. The Public Facing responses are those that can be included in the published report.

3. If you have any questions, 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, Performance, and Risk (005PR) at (202) 461-5139.

/s/ Dominic Cussatt

Attachment

Attachment

Office of Information and Technology
Comments to Draft OIG Report,
"Federal Information Security Modernization Act Audit for FY 2018"
OIG Recommendations and OIT Responses:

Recommendation 1: We recommended the Executive in Charge for Information and Technology consistently implement an agency-wide risk management governance structure, along with mechanisms to identify, monitor, and manage risks across the enterprise.

OIT Response: VA non-concurs with this recommendation. VA has aligned CSF and RMF to provide visibility into cybersecurity risk at the system-level and enterprise-level, which provides VA with the ability to analyze compliance, measure operational risk, and ultimately make risk-based determinations for an information system's Authority to Operate (ATO). Therefore, VA requests this finding be closed by OIG. Additional details regarding compensating activities to address the identified weaknesses have been provided to the IG.

Target Completion Date: Completed

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.

OIT Response: VA concurs with this recommendation. VA is in the process of developing and enhancing processes through oversight of VA information security compliance objectives. VA is tracking the implementation of the new GRC solution, as a project within the Enterprise Cybersecurity Strategy Program (ECSP) that will support remediation of weaknesses identified around the authorization lifecycle. Additional details regarding compensating activities to address the identified weaknesses have been provided to the IG.

Target Completion Date: 10/07/2019

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.

OIT Response: VA concurs with this recommendation. VA is expanding its Plan of Action and Milestone (POA&M) efforts to accurately document remediation efforts prior to POA&M closure through its Governance Risk and Compliance (GRC) tool. Furthermore, VA plans to implement an accountability model to hold stakeholders responsible for proper closure of POA&Ms. Additional details regarding compensating activities to address the identified weaknesses have been provided to the IG.

Target Completion Date: 10/07/2019 and Quarter 1 of FY20.

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.

OIT Response: VA concurs with this recommendation. VA is expanding its Plan of Action and Milestone (POA&M) process to consistently detect, evaluate, and monitor the current state of identified security weaknesses. Furthermore, VA plans to enforce creation and documentation of POA&Ms. Additional details regarding compensating activities to address the identified weaknesses have been provided to the IG.

Target Completion Date: 10/07/2019 and Quarter 1 of FY20

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.

OIT Response: VA concurs with this recommendation. The Case Management process provides a systematic approach for continuous evaluation of system security plans for identification of security controls as they apply to the current operational environment. Additional details regarding compensating activities to address the identified weaknesses have been provided to the IG.

Target Completion Date: 10/07/2019 and Quarter 1 of FY20

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.

OIT Response: VA concurs with this recommendation. VA is modifying its procedures for tracking deficient security controls that will provide a detailed view that highlights which security risks have been fully mitigated and which still require remediation. Additional details regarding compensating activities to address the identified weaknesses have been provided to the IG.

Target Completion Date: 10/07/2019 and Quarter 1 of FY20

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.

OIT Response: VA concurs with this recommendation. VA is currently taking measures to address the findings regarding service account password configuration and the service account password change process, based on deployment of the DHS CDM PAM solution. Additional details regarding compensating activities to address the identified weaknesses have been provided to the IG.

Target Completion Date: 3/26/2019

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.

OIT Response: VA concurs with this recommendation. VA is working with the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program to create a master user record (MUR). The MUR will pull-in data from multiple sources to build an access record for users at the VA network. In addition, VA is working on developing policy for financial applications, outlining annual user account reviews for adding, modifying and or deleting user accounts. Moreover, VA is working on developing a workflow to enforce proper completion of access request forms prior to assigning access / menus, which will allow VA to reproduce evidence within a database structure. VA is in the process of developing and implementing an enterprise-wide onboarding, monitoring and off-boarding solution referred to as the VA Onboarding Solution. Additional details regarding compensating controls to address the identified weaknesses have been provided to the IG.

Target Completion Date: 3/26/2019

Recommendation 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.

OIT Response: VA concurs with this recommendation. VA will continue to improve system owner accountability and communication with CSOC to ensure that audit logging for critical systems is performed. Additional details regarding compensating activities to address the identified weaknesses have been provided to the IG.

Target Completion Date: 0025: 9/25/2020, 0097: 1/25/2019

Recommendation 10: We recommended the Executive in Charge for Information and technology fully implement two-factor authentication to the extent feasible for all user accounts throughout the agency.

OIT Response: VA concurs with this recommendation. VA has taken necessary mitigations to reduce the risk to the enterprise by implementing compensating controls.

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.

OIT Response: VA concurs with this recommendation. VA Office of Information Security (OIS) commissioned the establishment of a centralized vulnerability management program office in FY18 to strengthen processes related to the identification, classification, remediation and mitigation of vulnerabilities throughout the enterprise. In addition, the agency is deploying a series of infrastructure enhancements through the DHS Continuous Diagnostics and Mitigation program that provide additional Information Security Continuous Monitoring tools to enable automated continuous assessment capabilities. VA is in the process of developing and implementing an enterprise-wide system per previous IG guidance. A vulnerability management program and a strategy for segregating medical devices to better protect sensitive information is in the process of being implemented. Additional details regarding compensating and mitigating activities to address the identified weaknesses have been provided to the IG.

Target Completion Date: 0002: In Progress, 0025: 9/25/2020, 0062: 3/18/2022, 0104: 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.

OIT Response: VA concurs with this recommendation. 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.

Target Completion Date: 08/09/2021

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.

OIT Response: VA concurs with this recommendation. VA is in the process of developing and implementing enhanced processes for security baseline creation, implementation, testing, and monitoring. Additional details regarding compensating and mitigating activities to address the identified weaknesses have been provided to the IG.

Target Completion Date: 03/01/2020

Recommendation 14: We recommended the Executive in Charge for Information and Technology implement improved network access controls to restrict medical devices from the general network and ensure that databases, file shares, and management devices, are adequately secured prior to connecting to VA's network.

OIT Response: VA concurs with this recommendation. VA has implemented an enterprise-wide system vulnerability management program and a strategy for segregating medical devices to better protect sensitive information is in the process of being implemented. Additional details regarding compensating and mitigating activities to address the identified weaknesses have been provided to the IG.

Target Completion Date: Completed

Recommendation 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.

OIT Response: VA concurs with this recommendation. Medical device cybersecurity is a shared responsibility between the device manufacturer and VA. Modification of these FDA (Food & Drug Administration) regulated devices requires written authorization from the manufacturer or the VA assumes full liability of the device. The VA's Special Device Security Division (SDSD) and VHA have implemented a continuous monitoring process to ensure the integrity and compliance of the MDIA ACLs and to ensure the continued provision of direct treatment, diagnostics, and monitoring of patient care by the VA's medical devices.

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.

OIT Response: VA concurs with this recommendation. VA Office of Information Security (OIS) commissioned the establishment of a centralized vulnerability management program office in FY-18 to strengthen processes related to the identification, classification, remediation and mitigation of vulnerabilities throughout the enterprise. In addition, the agency is deploying a series of infrastructure enhancements through the DHS Continuous Diagnostics and Mitigation program that provide additional Information Security Continuous Monitoring tools to enable automated continuous assessment capabilities. VA is in the process of developing and implementing an enterprise-wide system per previous IG guidance. A vulnerability management program and a strategy for segregating medical devices to better protect sensitive information is in the process of being implemented. Additional details regarding compensating and mitigating activities to address the identified weaknesses have been provided to the IG.

Target Completion Date: 09/30/2020

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.

OIT Response: VA concurs with this recommendation. VA is developing and implementing an enterprise-wide system to facilitate consistent change management of financial applications and networks. Additional details regarding compensating and mitigating activities to address the identified weaknesses have been provided to the IG.

Target Completion Date: 11/30/2021

Recommendation 18: We recommended the Executive in Charge for Information and Technology implement improved processes for ensuring that backup data is adequately secured in accordance with organizational policy.

OIT Response: VA non-concurs with this recommendation. VA has implemented measures to safely secure, store, and restore certain legacy backup tapes and request this finding be closed by OIG.

Target Completion Date: Completed

Recommendation 19: We recommended the Executive in Charge for Information and Technology implement improved processes for the review of system outages and disruptions for contingency plan improvements in accordance with defined policy.

OIT Response: VA non-concurs with this recommendation. The network and system outages / disruptions identified by OIG were deemed by VA as a minor outage / disruption which would not warrant the initiation of IT Contingency / Disaster Recovery (CP / DR) Plans, rather would be remediated via VA's ticketing system. After review of the list of outages that exceeded the 12-hour Recovery Time Objective (RTO), none of the outages reviewed affected critical systems and many were circuit outages affecting sites over the weekend when closed. However, the RTO is a number that is compared to the Maximum Tolerable Downtime (MTD), the customer states their MTD is 12 hours and OIT plans longest restoration time as 12 hours. For critical systems an incident call is started, and the customer is informed of the restoration steps. There is no NIST / FISMA requirement to always meet the target RTO and in these cases of non-critical outages, our actual enterprise CPs and DR plan was not utilized, as these were minor in nature. Moreover, lessons learned were not incorporated as part of the post-outages / disruptions follow-up, as the contingency plan was not initiated and would therefore not require an update to address any problems encountered during contingency plan implementation, executing, or testing, nor is incorporating lessons learned a requirement with VA Handbooks 6500/6500.8.

Target Completion Date: Completed

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.

OIT Response: VA concurs with this recommendation. VA is in the process of developing and implementing an enterprise-wide workflow to centralize the oversight and authorizing of MOU/ISA to determine completeness and quality. Additional details regarding compensating activities to address the identified weaknesses have been provided to the IG.

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.

OIT Response: VA concurs with this recommendation. VA CSOC continues to develop new processes and tracking of metrics to strengthen the agency-wide incident response process. Additional details regarding compensating activities to address the identified weaknesses have been provided to the IG.

Target Completion Date: 1/25/2019

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.

OIT Response: VA concurs with this recommendation. VA ITOPS and VA CSOC are working toward integrating the VA CSOC Splunk systems and QRADAR systems which will allow for improved visibility and monitoring, investigations, and adversarial hunting across the enterprise.

Target Completion Date: 1/25/2019

Recommendation 23: We recommended the Executive in Charge for Information and Technology implement improved safeguards to identify and prevent unauthorized vulnerability scans on VA networks.

OIT Response: VA concurs with this recommendation. ITOPS IO Cybersecurity Management is in the process of initiating a project to leverage the enterprise ForeScout infrastructure Threat Protection capabilities to identify unauthorized scanning across the enterprise. Additional details regarding compensating activities to address the identified weaknesses have been provided to the IG.

Target Completion Date: 7/29/2019

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

OIT Response: VA concurs with this recommendation. VA is in the process of evaluating enterprise tools to identify and prevent the use of unauthorized software on agency devices. Additional details regarding compensating and mitigating activities to address the identified weaknesses have been provided to the IG.

Target Completion Date: 06/28/2021

Recommendation 25. We recommended the Executive in Charge for Information and Technology develop a comprehensive inventory process to identify connected hardware, software, and firmware used to support VA programs and operations.

OIT Response: VA concurs with this recommendation. VA is in the process of developing enhanced processes to accurately inventory software and hardware across the enterprise. Additional details regarding compensating and mitigating activities to address the identified weaknesses have been provided to the IG.

Target Completion Date: 11/30/2021

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.

OIT Response: VA concurs with this recommendation. VA CSOC 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. Additional details regarding compensating activities to address the identified weaknesses have been provided to the IG.

Target Completion Date: 12/31/2019

Recommendation 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.

OIT Response: VA concurs with this recommendation. VA is in the process of improving mechanisms for system inventory management across the enterprise. Additional details regarding compensating and mitigating activities to address the identified weaknesses have been provided to the IG.

Target Completion Date: 11/30/2021

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.

OIT Response: VA concurs with this recommendation. VA is in the process of developing and implementing an enterprise-wide onboarding, monitoring and off-boarding solution referred to as the VA Onboarding Solution. Additional details regarding compensating to address the identified weaknesses have been provided to the IG. PSCM has procured Commercial Off-The-Shelf (COTS) product VA-CABS to serve as a VA-wide personnel security and suitability case management system. VA-CABS was deployed to the Security and Investigations Center (SIC) in September 2018. PSCM is also currently deploying VA-CABS incrementally across the enterprise. VA-CABS will monitor investigations and reinvestigations for timely actions. Servicing Human Resource Offices (SHRO) will be able to review their employee's investigation status and initiate reinvestigations as necessary. The SIC will continue to monitor contractors within VA and track their reinvestigation requirements with the Contracting Officer's Representative (COR). Initial training sessions have been conducted with CORs to obtain end-user insight and feedback on the VA Onboarding solution (which will integrate with VA-CABS) contractor onboarding and off-boarding functionalities. The Pilot has been paused to address process anomalies that were discovered. The Pilot is planning to resume in January 2019, testing the updated functionalities, prior to enterprise-wide release. Additional details regarding activities to address the identified findings have been provided to the IG.

Target Completion Date: In Progress

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 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.