DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

DEPARTMENT OF VETERANS AFFAIRS

Federal Information Security Modernization Act Audit for Fiscal Year 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.

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
OFFICE OF INSPECTOR GENERAL
WASHINGTON, DC 20001

MEMORANDUM

TO: Assistant Secretary for Information and Technology

FROM: Assistant Inspector General for Audits and Evaluations

SUBJECT: VA's Federal Information Security Modernization Act (FISMA) Audit for Fiscal Year 2019

1. Enclosed is the final audit report, *VA's Federal Information Security Modernization Act Audit for Fiscal Year 2019*. The Office of Inspector General (OIG) contracted with the independent public accounting firm, CliftonLarsonAllen LLP, to assess VA's information security program in accordance with FISMA.

2. To ensure the adequacy and effectiveness of information security controls, FISMA requires agency program officials, chief information officers, and inspectors general to conduct annual reviews of agencies' information security programs and report the results to the Department of Homeland Security (DHS). DHS uses these results 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) 2019. CliftonLarsonAllen LLP will follow up on the outstanding recommendations and evaluate the adequacy of corrective actions during its FY 2020 FISMA audit. According to findings by CliftonLarsonAllen LLP, VA continues to face significant challenges in complying with FISMA due to the nature and maturity of its information security program. VA therefore needs to implement improved controls. Specifically, VA should do the following:

   - Address security-related issues that contributed to the information technology material weakness reported in the FY 2019 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 mitigate significant security risks.

4. This report provides 25 recommendations for improving VA's information security program. Twenty-four 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. All 25 recommendations from last year's report on FISMA compliance remain open. Despite VA's commitment that the recommendations would be closed, some of them have been repeated for multiple years. VA successfully closed three recommendations in FY 2019 from prior years. Some recommendations were modified or not closed because information security control deficiencies were repeated during the FY 2019 FISMA audit.

5. The effect of the open recommendations will be considered in the FY 2020 assessment of VA's information security program. The OIG remains concerned that continuing delays in implementing effective corrective actions to address these open recommendations could contribute to reporting a material weakness in connection with VA's information technology security controls during the FY 2020 audit of the Department's consolidated financial statements.

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
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	plan of action and milestones
SCA	security control assessment

Inspector General
United States Department of Veterans Affairs
March 24, 2020

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, 2019. 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 Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions 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 24 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 2019 through October 2019.

Based on our audit procedures, we concluded that VA continues to face significant challenges meeting the requirements of FISMA. This report provides 25 recommendations to assist VA in strengthening its information security program.

In connection with the audit of VA's FY 2019 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 2019.

Our work did not include an assessment of the sufficiency of internal control over financial reporting or other matters not specifically outlined in the enclosed report. CLA cautions that projecting the results of our performance audit to future periods is subject to the risks that conditions may materially change from their current status. We concluded our fieldwork and assessment on October 1, 2019. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to October 1, 2019.

The purpose of this audit report is to report on our assessment of VA's compliance with FISMA and is not suitable for any other purpose.

Additional information on our findings and recommendations are included in the accompanying report. We are submitting this report to VA's Office of Inspector General.

CliftonLarsonAllen LLP

CliftonLarsonAllen LLP

Arlington, Virginia
March 24, 2020

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 2019 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 24 VA facilities. In FY 2019, 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 25 recommendations for improving VA's information security program: 24 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 information security control deficiencies were repeated during the FY 2019 FISMA audit. VA successfully closed three recommendations in FY 2019. The FY 2018 FISMA report provided 28 recommendations for improvement.

III.   Results and Recommendations

Agency-Wide Security Management Program

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

Progress Made While Challenges Remain

In FY 2019, VA's Chief Information Officer continued the Enterprise Cybersecurity Strategy Program (ECSP) to implement the VA Cybersecurity Strategy. Several initiatives have been launched, new tools have been implemented, and projects were actively being worked. However, issues remain with the consistent application of the security program and practices across VA's portfolio of systems. VA needs to ensure adequate control and risk management procedures are applied to all of their systems and applications in order to fully address previously identified weaknesses. The ECSP team has launched 31 high level action plans to address previously identified security weaknesses and the IT material weakness. As part of the ongoing ECSP efforts, we noted improvements related to:

- Improved security documentation
- Centralization of control functions
- Further maturation of predictive scanning process
- Enhanced boundary protections and network threat monitoring techniques
- 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 its enterprise wide risk and security management processes however, we continue to identify deficiencies related to overall governance to include risk and authorization processes, plans of action and milestones (POA&M), 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.

Risk Management Strategy

VA has not consistently 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, previously known or identified system security risks were not consistently documented in corresponding remediation plans or considered in risk management decisions. Additionally, VA's security control assessment process did not ensure that assessment teams were adequately independent from the systems under review and assessments did not fully evaluate the effectiveness of security controls. We also identified several instances of systems that 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. Additionally, the Risk Management Framework requires that security control assessments are performed by groups or individuals that are free from any conflicts of interest with respect to the development, operation, or management of the information system.

VA has implemented a risk governance structure, including a Risk Management Governance Board, to monitor system security risks and implement risk mitigation controls across the enterprise. Additionally, VA has begun transitioning IT systems to a new Governance, Risk and Compliance tool, entitled the Enterprise Mission Assurance Support System, to improve the process for assessing, authorizing, and monitoring the security posture of the agency. However, this effort was not fully completed at the end of our fieldwork.

Plans of Action and Milestones

OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, defines management and reporting requirements for agency POA&Ms, to include deficiency descriptions, remediation actions, required resources, and responsible parties. According to VA's central reporting database, the Department had approximately 10,507 open POA&Ms in FY 2019, as compared with 11,734 open POA&Ms in FY 2018. 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.

While VA has made progress in addressing previously identified security weaknesses, 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, and (c) POA&Ms were not consistently updated to consider all known security weaknesses.

POA&M deficiencies resulted from a lack of accountability for establishing, tracking, and closing items at a "local" or "system" level and a lack of controls to ensure supporting documentation was recorded in the repository tool. More specifically, system stewards and Information System Security Officers did not always ensure that adequate justification was established prior to closing POA&Ms. Additionally, control weaknesses identified during security control assessments were not always established as POA&Ms in accordance with set policy. System stewards and Information System Security Officers are ultimately responsible for these POA&M processes, however, they were not performing these duties in a consistent manner. By failing to fully remediate significant system security risks in the near term, VA management cannot ensure that information security controls will adequately protect VA systems throughout their life cycles. Further, without sufficient documentation in the central database to justify closure of POA&Ms, VA cannot ensure that corresponding security risks have been fully mitigated.

System Security Plans

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 was not addressed within regional level system security plans.

CORRECTIVE ACTIONS RECOMMENDED

1. We recommended the Assistant Secretary for Information and Technology consistently implement an improved continuous monitoring program in accordance with the NIST Risk Management Framework. Specifically, implement an independent security control assessment process to evaluate the effectiveness of security controls prior to granting authorization decisions. *(This is a modified repeat recommendation from prior years.)*

2. We recommended the Assistant Secretary for Information and Technology implement improved mechanisms to ensure system stewards and information system security officers follow procedures for establishing, tracking, and updating Plans of Action and Milestones for all known risks and weaknesses including those identified during security control assessments. *(This is a modified repeat recommendation from prior years.)*

3. We recommended the Assistant Secretary for Information and Technology implement controls to ensure that system stewards and responsible officials obtain appropriate documentation prior to closing Plans of Action and Milestones. *(This is a modified repeat recommendation from prior years.)*

4. We recommended the Assistant Secretary 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.)*

5. We recommended the Assistant Secretary for Information and Technology implement improved processes for reviewing and updating key security documents such as security plans and interconnection agreements 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 Assistant Secretary for Information and Technology concurred with Recommendations 1, 2, 3, 4, and 5. For Recommendation 1, the Assistant Secretary stated that VA follows the NIST Risk Management Framework and implements this as an assessment workflow in Enterprise Mission Assurance Support Service for effectiveness of security controls and requested this finding be closed by the Office of Inspector General (OIG). Additional details regarding compensating activities to address the identified weaknesses have been provided to the OIG. To address Recommendation 2, VA will continue to expand its Plan of Action and Milestone process to consistently detect, evaluate, and monitor the current state of identified potential security weaknesses. Additional details regarding compensating activities to address the identified weaknesses have been provided to the OIG. For Recommendation 3, VA states that prior to the Enterprise Mission Assurance Support Service, VA maintained the same capability within Risk Vision to ensure its Plans of Action and Milestones were managed consistent with the POA&M Management Guide. Additional details regarding compensating activities to address the identified weaknesses have been provided to the OIG. For Recommendation 4, VA has implemented measures to document and report risk to the overall cybersecurity risk management approach that informs security and risk-based decisions across its information system environment and requested this finding be closed by the OIG. Additional details regarding activities to address the identified findings have been provided to the OIG. To address Recommendation 5, VA provided training to system stakeholders regarding updates made to Memoranda of Understanding/Interconnection Security Agreement Standard Operating Procedures and requested this finding be closed by the OIG. Additional details regarding compensating activities to address the identified weaknesses have been provided to the OIG.

OIG Response

The Assistant Secretary for Information and Technology's planned corrective actions are responsive to Recommendations 1, 2, 3, 4, and 5. VA requested closure for Recommendations 1, 4, and 5. The OIG will evaluate the requests for closure during the FY 2020 FISMA audit. Additionally, 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 Assistant Secretary's comments.

Identity Management and Access Controls

We continued to identify significant deficiencies with 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 several areas

including password management, access management, audit logging and monitoring, and strong authentication controls.

A. Password Management

The audit team 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. Specifically, we noted that security logs were not always enabled, effectively managed, aggregated, or proactively reviewed for certain significant systems, such as Veterans 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 during FY 2019. VA Handbook 6500, Appendix F establishes high-level policy and procedures for managing system connections and authentication standards. Moving forward, VA needs to fully implement strong authentication for all users before connecting to VA networks.

CORRECTIVE ACTIONS RECOMMENDED

6. We recommended the Assistant Secretary for Information and Technology implement improved processes to ensure compliance with VA password policy and security standards on domain controls, operating systems, databases, applications, and network devices. *(This is a repeat recommendation from prior years.)*

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

8. We recommended the Assistant Secretary 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.)*

9. We recommended the Assistant Secretary for Information and Technology fully implement two-factor authentication to the extent feasible for all user accounts throughout the agency. *(This is a repeat recommendation from prior years.)*

Management Comments

The Assistant Secretary for Information and Technology concurred with Recommendations 6, 7, 8, and 9. For Recommendation 6, the Assistant Secretary stated that VA is transitioning service accounts for centralized management. Additional details regarding activities to address the identified finding have been provided to the OIG. For Recommendation 7, 8 and 9, the Assistant Secretary stated additional details regarding activities to address the identified findings have been provided to the OIG.

OIG Response

The Assistant Secretary for Information and Technology's planned corrective actions are responsive to Recommendations 6, 7, 8, and 9. 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 Assistant Secretary's comments.

Configuration Management Controls

We continued to identify significant deficiencies with 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 security control deficiencies related to unsecure web application servers, excessive permissions on database platforms, vulnerable and unsupported 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 consistently 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 unauthorized access permissions to critical system information. We also noted that VA did not have a complete inventory of databases for various locations throughout the enterprise. 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 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

VA made progress in developing access control lists to segment medical devices using the Medical Device Isolation Architecture. However, network vulnerability assessments identified instances where the segmentation was not appropriately designed or configured to prevent the detection of lessor secured medical devices. Weak network segmentation controls 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 segmented from other networks. Numerous critical and high-risk vulnerabilities, such as excessive system permissions, were identified on unpatched systems that support medical devices 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 and (2) insecure database configuration privileges.

We also 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 facilities. Consequently, some networks not controlled by OIT had significant vulnerabilities that weakened the overall security posture of the local facilities. VA's Enterprise Program Management Office and other offices were responsible for securing systems that are not managed by OIT. By not implementing more 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.

CORRECTIVE ACTIONS RECOMMENDED

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

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

12. We recommended the Assistant Secretary 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.)*

13. We recommended the Assistant Secretary for Information and Technology implement improved network access controls that restrict medical devices from systems hosted on the general network. *(This is a modified repeat recommendation from prior years.)*

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

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

Management Comments

The Assistant Secretary for Information and Technology concurred with Recommendations 10, 11, 12, 13, 14, and 15. For Recommendations 10, 11, 12, 13, 14, and 15, the Assistant Secretary stated additional details regarding activities to address the identified findings have been provided to the OIG.

OIG Response

The Assistant Secretary for Information and Technology's planned corrective actions are responsive to Recommendations 10, 11, 12, 13, 14, and 15. 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 Assistant Secretary's comments.

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. VA has implemented a new change management system, which has the capability of requiring certain artifacts to be completed before changes are approved and implemented. This requirement was not in place for the legacy systems. By not enforcing a standardized change control methodology, system development projects may be inconsistently developed, tested, and migrated into production, thereby placing VA systems at risk of unauthorized or unintended software modifications.

CORRECTIVE ACTION RECOMMENDED

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

Management Comments

The Assistant Secretary for Information and Technology concurred with Recommendation 16. For Recommendation 16, the Assistant Secretary stated additional details regarding activities to address the identified finding have been provided to the OIG.

OIG Response

The Assistant Secretary for Information and Technology's planned corrective actions are responsive to Recommendation 16. 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 Assistant Secretary's comments.

Contingency Planning

VA contingency plans provide high level recovery objectives for systems and operations in the event of disruption or disaster. However, we noted that VA did not consistently meet these recovery objectives throughout the year. Additionally, contingency plans did not always include all required information. 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:

- Major incidents were not always resolved within stated Recovery Time Objectives. We noted several instances throughout the year of system or service outages that were not restored in accordance with internal VA goals.

- We also observed instances of system contingency plans that did not include sufficient information related to the system boundary including the identification of critical assets and system components. Additionally, the plans did not always consider interdependencies with other system and platform boundaries.

VA established standard recovery goals and procedures for their large system boundaries, which makes it difficult to recover all systems and operations within stated objectives. If business functions are not recovered within agreed upon timeframes, VA is at risk of not adequately providing mission-critical services in a consistent and resilient manner.

CORRECTIVE ACTIONS RECOMMENDED

17. We recommended the Assistant Secretary for Information and Technology review system boundaries, recovery priorities, system components, and system interdependencies and implement appropriate mechanisms to ensure that established system recovery objectives are met. *(This is a modified repeat recommendation from prior years.)*

Management Comments

The Assistant Secretary for Information and Technology concurred with Recommendation 17. For Recommendation 17, the Assistant Secretary stated additional details regarding activities to address the identified findings have been provided to the OIG.

OIG Response

The Assistant Secretary for Information and Technology'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 Assistant Secretary's comments.

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 Internal Network Segments Not Monitored

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. We identified these issues at several medical facilities and data centers throughout the year. 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. Various data feeds were added throughout the year but the VA environment is large and complex and changes frequently. Without adequate coverage of monitoring tools, VA is at risk of not identifying or preventing potential security events. 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 four 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 instances of security events that were not reported as incident tickets within the timeframes required by VA Handbook 6500. The responsibility for establishing incident tickets is a shared responsibility between the Cybersecurity Operations Center and the Information System Security Officers in the field. Although training and education is regularly provided, the Information System Security Officers did not consistently follow the requirements for reporting suspected incidents in a timely manner. If incidents are not effectively established and tracked, VA is at risk of not being able to appropriately respond to valid security events.

CORRECTIVE ACTIONS RECOMMENDED

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

19. We recommended the Assistant Secretary 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.)*

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

Management Comments

The Assistant Secretary for Information and Technology concurred with Recommendations 18, 19, and 20. For Recommendations 18, 19, and 20, the Assistant Secretary stated additional details regarding activities to address the identified findings have been provided to the OIG.

OIG Response

The Assistant Secretary for Information and Technology's planned corrective actions are responsive to Recommendations 18, 19, and 20. 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 Assistant Secretary's comments.

Continuous Monitoring

Although progress has been made, VA lacks a consistent 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 system owners and Information System Security Officers for each system and application. VA completed numerous security control assessments throughout the year utilizing a standardized methodology and approach. However, we identified inconsistencies with how assessment results 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, we identified several instances of security control deficiencies that were consolidated under one control when the underlying security issues should have been tracked separately within individual POA&Ms. Furthermore, we noted that certain security control deficiencies were not always formally tracked and reported in accordance with set policy. Consequently, the POA&M process did not effectively communicate or track the breadth and depth of the security risks affecting mission critical systems.

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 Strategy* 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 and continued to implement additional tools and measures as part of the ongoing DHS Continuous Diagnostics and Mitigation program. 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.

CORRECTIVE ACTIONS RECOMMENDED

21. We recommended the Assistant Secretary for Information and Technology implement improved measures to ensure that security control deficiencies are tracked individually instead of consolidating security deficiencies under one control. *(This is a modified repeat recommendation from prior years.)*

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

23. We recommended the Assistant Secretary 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 repeat recommendation from prior years.)*

Management Comments

The Assistant Secretary for Information and Technology concurred with Recommendations 21, 22, and 23. For Recommendations 21, 22, and 23, the Assistant Secretary stated additional details regarding activities to address the identified findings have been provided to the OIG.

OIG Response

The Assistant Secretary for Information and Technology's planned corrective actions are responsive to Recommendations 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 Assistant Secretary's comments.

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 2019. Specifically:

- VA did not have consistent processes in place to review control assessments such as Statement on Standards for Attestation Engagements 18 reports for contractor managed systems and ensure Common User Entity Controls were in place. These reports provide organizations valuable information and assurances regarding the effectiveness of the service provider's control environment.

- We identified significant control weaknesses on contractor managed systems such as HR Smart and the Vendor Resource Management System.

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

CORRECTIVE ACTIONS RECOMMENDED

24. We recommended the Assistant Secretary for Information and Technology implement improved procedures for monitoring contractor-managed systems and services and ensure information security controls adequately protect VA sensitive systems and data. *(This is a modified repeat recommendation from prior years.)*

Management Comments

The Assistant Secretary for Information and Technology concurred with Recommendation 24. For Recommendation 24, the Assistant Secretary stated additional details regarding activities to address the identified findings have been provided to the OIG.

OIG Response

The Assistant Secretary for Information and Technology's planned corrective actions are responsive to Recommendation 24. 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 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. FISMA audits continue to identify issues related to timeliness of background investigations.

Management Comments

The Assistant Secretary for Information and Technology concurred with Recommendation FY 2006-04. The Assistant Secretary stated additional details regarding activities to address the identified findings have been provided to the OIG.

OIG Response

The Assistant Secretary for Information and Technology'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 recommendation until all proposed actions are completed. Appendix D provides the full text of the 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 2018, OMB issued Memorandum M-19-02, *Fiscal Year 2018-2019 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 2019 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 2019. 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 24 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 2019 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 Medical Facility—Bronx, NY

- VA Medical Facility—Fargo, ND

- VA Regional Office—Fargo, ND

- VA Medical Facility—Fayetteville, NC

- VA Medical Facility—Helena, MT

- VA Medical Facility—Hines, IL

- Information Technology Center—Hines, IL

- VA Medical Facility—Iowa City, IA

- VA Medical Facility—Jackson, MS

- Network Security Operations Center—Martinsburg, WV

- Capital Region Readiness Center—Martinsburg, WV

- VA Medical Facility—Memphis, TN

- VA Medical Facility—Minneapolis, MN

- VA Regional Office—Minneapolis, MN

- VA Medical Facility—Nashville, TN

- VA Regional Office—Nashville, TN

- Information Technology Center—Philadelphia, PA

- Loan Guaranty Contractor Managed Facility—Plano, TX

- National Cemetery Administration—Quantico, VA

- VA Medical Facility—Sacramento, CA

- VA Central Office—Washington, DC

- VA Medical Facility—Wilkes Barre, PA

- VA Enterprise Cloud—Virtual

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 Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix D: Assistant Secretary for Information and Technology Comments

Department of Veterans Affairs

Memorandum

Date: February 24, 2020

From: Assistant Secretary for Information and Technology and Chief Information Officer (005)

Subj: Draft OIG Report: Federal Information Security Management Act (FISMA) Assessment for FY 2019

To: Assistant Inspector General for Audits and Evaluations

1. The Department of Veterans Affairs (VA) appreciates the opportunity to respond to the Office Inspector General's (OIG) draft report, *Federal Information Security Management Act Audit for Fiscal Year 2019.* VA is currently developing various projects to correct the items found in the Fiscal Year 2019 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. Should you have any questions regarding the responses, please contact Martha K. Orr, Deputy Chief Information Officer for Quality, Privacy, and Risk at (202) 461-5139.

/s/ James G. Gfrerer

Attachment

Federal Information Security Modernization Act (FISMA) Audit for Fiscal Year 2019
OIT Response to Draft OIG Report

Agency-Wide Security Management Program

Recommendation 1: We recommended the Assistant Secretary for Information and Technology consistently implement an improved continuous monitoring program in accordance with the NIST Risk Management Framework. Specifically, implement an independent security control assessment process to evaluate the effectiveness of security controls prior to granting authorization decisions. (This is a modified repeat recommendation from prior years.)

OIT Response: VA concurs with this recommendation. VA follows National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and implements this as an assessment workflow in Enterprise Mission Assurance Support Service (eMASS) for effectiveness of security controls and requests this finding be closed by the Office of the Inspector General (OIG). Additional details regarding compensating activities to address the identified weaknesses have been provided to the Inspector General (IG).

Target Completion Date: Completed.

Recommendation 2: We recommended the Assistant Secretary for Information and Technology implement improved mechanisms to ensure system stewards and information system security officers follow procedures for establishing, tracking, and updating Plans of Action and Milestones for all known risks and weaknesses including those identified during security control assessments. (This is a modified repeat recommendation from prior years.)

OIT Response: VA concurs with this recommendation. VA will continue to expand its Plan of Action and Milestone (POA&M) process to consistently detect, evaluate, and monitor the current state of identified potential security weaknesses. Additional details regarding compensating activities to address the identified weaknesses have been provided to the Inspector General (IG).

Target Completion Date: The estimated time of completion (EOC) for the accountability structure is 3rd Quarter 2020.

Recommendation 3: We recommended the Assistant Secretary for Information and Technology implement controls to ensure that system stewards and responsible officials obtain appropriate documentation prior to closing Plans of Action and Milestones. (This is a modified repeat recommendation from prior years.)

OIT Response: VA concurs with this recommendation. Prior to the Enterprise Mission Assurance Support Service (eMASS), VA maintained the same capability within Risk Vision (RV) to ensure its Plans of Action and Milestones (POA&M) were managed consistent with the POA&M Management Guide. Additional details regarding compensating activities to address the identified weaknesses have been provided to the Inspector General (IG).

Target Completion Date: The estimated time of completion (EOC) for the accountability structure is 3rd Quarter 2020.

Recommendation 4: We recommended the Assistant Secretary 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.)

OIT Response: VA concurs with this recommendation. VA implements measures to document and report risk to the overall cybersecurity risk management approach that informs security and risk-based decisions across its information system environment and requests this finding be closed by the OIG. Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).

Target Completion Date: Completed.

Recommendation 5: We recommended the Assistant Secretary for Information and Technology implement improved processes for reviewing and updating key security documents such as security plans and interconnection agreements on an annual basis and ensure the information accurately reflects the current environment. (This is a modified repeat recommendation from prior years.)

OIT Response: VA concurs with this recommendation. VA provided training to system stakeholders regarding updates made to Memoranda of Understanding (MOU)/Interconnection Security Agreement (ISA) Standard Operating Procedures (SOPs) and requests this finding to be closed by the OIG. Additional details regarding compensating activities to address the identified weaknesses have been provided to the Inspector General (IG).

Target Completion Date: Completed.

Identity Management and Access Controls

Recommendation 6: We recommended the Assistant Secretary for Information and Technology implement improved processes to ensure compliance with VA password policy and security standards on domain controls, operating systems, databases, applications, and network devices. (This is a repeat recommendation from prior years.)

OIT Response: VA concurs with this recommendation. VA is transitioning service accounts for centralized management. Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).

Target Completion Date: The estimated time of completion (EOC) is 5/21/2023.

Recommendation 7: We recommended the Assistant Secretary for Information and Technology implement periodic reviews to minimize access by system users with incompatible roles, permissions in excess of required functional responsibilities, and unauthorized accounts. (This is a repeat recommendation from prior years.)

OIT Response: VA concurs with this recommendation. Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).

Target Completion Date: The estimated time of completion (EOC) is 5/21/2023.

Recommendation 8: We recommended the Assistant Secretary 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.)

OIT Response: VA concurs with this recommendation. Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).

Target Completion Date: The estimated time of completion (EOC) is 9/30/2021.

Recommendation 9: We recommended the Assistant Secretary for Information and Technology fully implement two-factor authentication to the extent feasible for all user accounts throughout the agency. (This is a repeat recommendation from prior years.)

OIT Response: VA concurs with this recommendation. Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).

Target Completion Date: The estimated time of completion (EOC) is 03/31/2022.

Configuration Management Controls

Recommendation 10: We recommended the Assistant Secretary for Information and Technology implement more effective automated mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and web application servers. (This is a repeat recommendation from prior years.)

OIT Response: VA concurs with this recommendation. Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).

Target Completion Date: The estimated time of completion (EOC) is 10/01/2021.

Recommendation 11: We recommended the Assistant Secretary for Information and Technology implement a more effective patch and vulnerability management program to address security deficiencies identified during our assessments of VA's web applications, database platforms, network infrastructure, and workstations. (This is a repeat recommendation from prior years.)

OIT Response: VA concurs with this recommendation. Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).

Target Completion Date: The estimated time of completion (EOC) is 10/01/2021.

Recommendation 12: We recommended the Assistant Secretary 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.)

OIT Response: VA concurs with this recommendation. Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).

Target Completion Date: The estimated time of completion (EOC) is 10/30/2020.

Recommendation 13: We recommended the Assistant Secretary for Information and Technology implement improved network access controls that restrict medical devices from systems hosted on the general network. (This is a modified repeat recommendation from prior years.)

OIT Response: VA concurs with this recommendation. Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).

Target Completion Date: The estimated time of completion (EOC) is 12/31/2021.

Recommendation 14: We recommended the Assistant Secretary for Information and Technology consolidate the security responsibilities for networks not managed by the Office of Information and Technology, under a common control for each site and ensure vulnerabilities are remediated in a timely manner. (This is a repeat recommendation from prior years.)

OIT Response: VA concurs with this recommendation. Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).

Target Completion Date: The estimated time of completion (EOC) is 08/06/2022.

Recommendation 15: We recommended the Assistant Secretary for Information and Technology implement improved processes to ensure that all devices and platforms are evaluated using credentialed vulnerability assessments. (This is a repeat recommendation from prior years.)

OIT Response: VA concurs with this recommendation. Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).

Target Completion Date: The estimated time of completion (EOC) is 08/06/2022.

System Development and Change Management Controls

Recommendation 16: We recommended the Assistant Secretary for Information and Technology implement improved procedures to enforce standardized system development and change control processes that integrates information security throughout the life cycle of each system. (This is a repeat recommendation from prior years.)

OIT Response: VA concurs with this recommendation. Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).

Target Completion Date: The estimated time of completion (EOC) is 04/20/2020.

Contingency Planning

Recommendation 17 We recommended the Assistant Secretary for Information and Technology review system boundaries, recovery priorities, system components, and system interdependencies and implement appropriate mechanisms to ensure that established system recovery objectives are met. (This is a modified repeat recommendation from prior years.)

OIT Response: VA concurs with this recommendation. Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).

Target Completion Date: None.

Incident Response and Monitoring

Recommendation 18: We recommended the Assistant Secretary for Information and Technology implement more effective agency-wide incident response procedures to ensure timely notification, reporting, updating, and resolution of computer security incidents in accordance with VA standards. (This is a repeat recommendation from prior years.)

OIT Response: VA concurs with this recommendation. Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).

Target Completion Date: The estimated time of completion (EOC) is 03/01/2021.

Recommendation 19: We recommended the Assistant Secretary 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.)

OIT Response: VA concurs with this recommendation. Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).

Target Completion Date: The estimated time of completion (EOC) is 09/30/2021.

Recommendation 20: We recommended the Assistant Secretary for Information and Technology implement improved safeguards to identify and prevent unauthorized vulnerability scans on VA networks. (This is a repeat recommendation from prior years.)

OIT Response: VA concurs with this recommendation. Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).

Target Completion Date: Complete.

Continuous Monitoring

Recommendation 21: We recommended the Assistant Secretary for Information and Technology implement improved measures to ensure that security control deficiencies are tracked individually instead of consolidating security deficiencies under one control. (This is a modified repeat recommendation from prior years.)

OIT Response: VA concurs with this recommendation. Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).

Target Completion Date: The estimated time of completion (EOC) for the accountability structure is 3rd Quarter 2020.

Recommendation 22: We recommended the Assistant Secretary for Information and Technology fully develop a comprehensive list of approved and unapproved software and implement continuous monitoring processes to prevent the use of prohibited software on agency devices. (This is a repeat recommendation from prior years.)

OIT Response: VA concurs with this recommendation. Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).

Target Completion Date: The estimated time of completion (EOC) for the accountability structure is 09/30/2022.

Recommendation 23: We recommended the Assistant Secretary 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 repeat recommendation from prior years.)

OIT Response: VA concurs with this recommendation. Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).

Target Completion Date: The estimated time of completion (EOC) for the accountability structure is 11/30/2021.

Contractor Systems Oversight

Recommendation 24: We recommended the Assistant Secretary for Information and Technology implement improved procedures for monitoring contractor-managed systems and services and ensure information security controls adequately protect VA sensitive systems and data. (This is a modified repeat recommendation from prior years.)

OIT Response: VA concurs with this recommendation. Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).

Target Completion Date: The estimated time of completion (EOC) for the accountability structure is 5/21/2023

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. Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).

Target Completion Date: The estimated time of completion (EOC) for the accountability structure is 12/31/2020

For accessibility, the original format of this appendix has been modified to comply with Section 508 of the Rehabilitation Act of 1973, as amended.

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.