



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 2021

AUDIT

REPORT #21-01309-74

APRIL 13, 2022



MISSION

The mission of the Office of Inspector General is to serve veterans and the public by conducting meaningful independent oversight of the Department of Veterans Affairs.

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.

FOR MORE
VA OIG REPORTS
CLICK HERE



**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/Chief Information Officer
FROM: Assistant Inspector General for Audits and Evaluations
SUBJECT: VA's Federal Information Security Modernization Act (FISMA) Audit for Fiscal Year (FY) 2021

1. Enclosed is the final report, *VA's Federal Information Security Modernization Act Audit for Fiscal Year 2021*. The VA 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 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 FY 2021. CliftonLarsonAllen LLP will follow up on the outstanding recommendations and evaluate the adequacy of corrective actions during its FY 2022 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. Therefore, VA 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 2021 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 26 recommendations for improving VA's information security program. The FY 2020 FISMA report also provided 26 recommendations for improvement. Some recommendations were modified or not closed because relevant information security control deficiencies identified during the FY 2021 FISMA audit were repeat deficiencies. Despite VA's commitment to close the recommendations, some of them have been repeated for multiple years.
 5. The effect of the open recommendations will be considered in the FY 2022 audit 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 2022 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
OIG	Office of Inspector General
OIT	Office of Information and Technology
OMB	Office of Management and Budget
POA&M	plans of action and milestones



CliftonLarsonAllen LLP
CLAconnect.com

March 16, 2022

Inspector General
United States Department of Veterans Affairs

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 (FY) ended September 30, 2021. 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 of 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 VA's 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 50 selected major applications and general support systems hosted at 24 VA facilities and on the VA Enterprise Cloud 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 2021 through October 2021.

Based on our audit procedures, we concluded that VA continues to face significant challenges meeting the requirements of FISMA. This report provides 26 recommendations to assist VA in strengthening its information security program.

In connection with the audit of VA's FY 2021 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 2021.



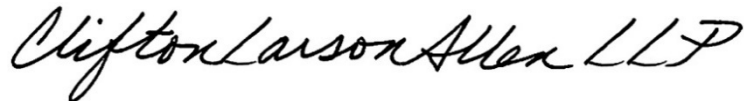
CLA is an independent member of Nexia International, a leading, global network of independent accounting and consulting firms. See nexia.com/member-firm-disclaimer for details.

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 November 3, 2021. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to November 3, 2021.

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 is included in the accompanying report. We are submitting this report to VA's Office of Inspector General.

CliftonLarsonAllen LLP

A handwritten signature in cursive script that reads "CliftonLarsonAllen LLP".

Arlington, Virginia
March 16, 2022

Table of Contents

I.	Objective	1
II.	Overview	1
III.	Results and Recommendations.....	2
	1. <i>Agency-Wide Security Management Program</i>	2
	2. <i>Identity Management and Access Controls</i>	5
	3. <i>Configuration Management Controls</i>	8
	4. <i>System Development and Change Management Controls</i>	11
	5. <i>Contingency Planning</i>	12
	6. <i>Incident Response and Monitoring</i>	14
	7. <i>Continuous Monitoring</i>	16
	8. <i>Contractor Systems Oversight</i>	18
	Appendix A: Status of Prior Year Recommendations	20
	Appendix B: Background.....	21
	Appendix C: Scope and Methodology	23
	Appendix D: Assistant Secretary for Information and Technology Comments.....	25
	Report Distribution	32

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 of 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 2021 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 50 major applications and general support systems at 24 VA facilities and on the VA Enterprise Cloud. In FY 2021, 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 and Change Management Controls
5. Contingency Planning
6. Incident Response and Monitoring
7. Continuous Monitoring
8. Contractor Systems Oversight

This report provides 26 recommendations for improving VA's information security program. Some recommendations were modified or not closed because relevant information security control deficiencies identified during the FY 2021 FISMA audit were repeat deficiencies. The FY 2020 FISMA report provided 26 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 2021, VA's Acting Chief Information Officer continued the Enterprise Cybersecurity Strategy Program (ECSP) to implement the VA Cybersecurity Strategy (VA issued a new cybersecurity strategy after FY 2021). 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 several high-level action plans to address previously identified security weaknesses and the IT material weakness reported as part of the Consolidated Financial Statement Audit. As part of the ongoing ECSP efforts, we noted improvements related to:

- Centralization of control functions.
- Further maturation of the predictive scanning process and remediation of newer vulnerabilities.
- New tools and software implemented to improve change management and the timeliness of background investigations.
- 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 comprehensive 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 and enforcement 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 systems and applications. 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 management processes, Plans of Action and Milestones (POA&M), and system security plans. 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

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. Security artifacts such as Risk Assessments and POA&Ms were also not documented in accordance with VA policies. 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 address all required controls or fully evaluate the effectiveness of security controls. We also identified several instances of systems that were granted Authority to Operate without undergoing an independent assessment of security controls.

NIST Special Publication (SP) 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, 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, in 2020, VA transitioned their IT systems portfolio and the associated security documentation 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 tool and the required procedures for completing security documentation were still being operationalized and matured during FY 2021 and we noted inconsistencies with the implementation of set procedures throughout the audit cycle.

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 25,821 ongoing POA&M items in FY 2021, as compared with 15,826 open POA&Ms in FY 2020. This increase can be largely attributed to the boundary re-organization that took place before FY 2020. This reorganization increased VA's overall inventory from roughly 280 systems and applications to over 700 unique systems in the FISMA inventory. 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 were not consistently documented in accordance with standards and policies, (b) POA&Ms that lacked sufficient documentation to justify closure, 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 documented. VA recently implemented a new Governance, Risk, and Compliance tool to enhance their security management documentation; however, the new processes and templates associated with the tool need time to mature and artifacts were not consistently documented according to VA standards. Inadequate security documentation may result in insufficient awareness and management of system risks and deficiencies as well as ineffective continuous monitoring of security controls.

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 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 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 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, risk assessments, and interconnection agreements on an annual basis and ensure the information accurately reflects the current environment. *(This is a repeat recommendation from prior years.)*

Management Comments

The Assistant Secretary for Information and Technology concurred with recommendations 1, 2, 4, and 5 and partially concurred with recommendation 3. For recommendation 1, the Assistant Secretary reported that the Office of Information Security will expand the number of systems undergoing the control review risk mitigation activity and iteratively address lessons learned to refine the process. To address recommendation 2, the Office of Information Technology will continue to hold updated Governance, Risk and Compliance tool trainings that support end users' responsibility and understanding of Plan of Action and Milestone processes, providing hands-on demonstrations of required processes in the tool. For recommendation 3, the Assistant Secretary reported VA partially concurs with the recommendation, stating that VA concurs that system stakeholders are not following the prescribed procedure for obtaining appropriate documentation prior to closing Plans of Action and Milestones. However, he stated mitigating controls are in place to reduce the risk when documentation is not initially closing the plans appropriately. To address recommendation 4, the Office of Information Security is working on a technical solution to ensure implementation details be populated prior to submission of system security plans. For recommendation 5, the Office of Information Technology will finalize accountability measures for stakeholders to perform quantitative reviews on key security documentation to remain compliant with VA policy.

OIG Response

The Assistant Secretary for Information and Technology's planned corrective actions are responsive to recommendations 1, 2, 3, 4, and 5. 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. The VA Knowledge Service 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 personnel investigations.

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. Specifically, numerous service accounts were identified that were not needed or had passwords that were not changed in over three years. 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. The VA Knowledge Service establishes password management standards for authenticating VA system users.

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

Access Management

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. The VA Knowledge Service 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. Furthermore, monitoring of access for individuals with elevated application privileges was lacking within several major application's production environments. This occurred because VA has not implemented effective reviews to monitor for instances of unauthorized system access or excessive permissions. Periodic reviews are critical to restrict legitimate users to specific systems and to prevent unauthorized access by both internal and external users. Unauthorized access to critical systems can leave sensitive data vulnerable to inappropriate modification or destruction.

Audit Logging and Monitoring

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 significant systems such

as Veterans Information Systems and Technology Architecture. These issues occurred because many systems and applications do not readily communicate with logging software or do not have the capability to produce comprehensive security logs. The VA Knowledge Service 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.

Personnel Screening and Investigations

VA's system of record for background investigations was inaccurate. In addition, some personnel did not receive the proper level of investigation for their position sensitivity levels. Furthermore, the centralized method for monitoring the investigation status of contractors was newly implemented and did not track all contractors. VA has begun the process of modernizing their infrastructure that supports the background investigation processes but that modernization takes time to mature and be fully implemented. Without accurate and reliable background investigation data, VA is at risk of allowing unnecessary or unauthorized access to sensitive systems and data.

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 Office of Personnel Security, Human Resources, and Contract Offices implement improved processes for establishing and maintaining accurate data within VA's authoritative system of record for background investigations. *(This is a modified repeat recommendation from prior years.)*
10. We recommended the Office of Personnel Security, Human Resources, and Contract Offices strengthen processes to ensure appropriate levels of background investigations are completed for applicable VA employees and contractors. *(This is a modified repeat recommendation from prior years.)*

Management Comments

The Assistant Secretary for Information and Technology concurred with recommendations 6, 7, 8, 9, and 10. For all the recommendations, the Assistant Secretary reported additional details regarding activities to address the identified findings have been provided to the OIG contracted auditors.

OIG Response

The Assistant Secretary for Information and Technology's planned corrective actions are responsive to recommendations 6, 7, 8, 9, and 10.¹ 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. The VA Knowledge Service 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.

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.

While VA has implemented a new process to identify web-based vulnerabilities, such as Structured Query Language injection attacks on major systems, the process for documenting, tracking, and remediation of those vulnerabilities was not yet formalized. Consequently, we continue to identify significant security vulnerabilities on web applications hosted at local facilities.

¹ Detailed activities to address the identified findings were provided to the Inspector General. The OIG removed information that is considered sensitive prior to publication.

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. NIST SP 800-160, Volume 2, *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, states that agencies should design, architect, and develop systems with the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises. 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.

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 remediate security weaknesses associated with outdated third-party applications or operating system software in a timely manner.

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.

Unsecure Network Access Controls

VA continued to make 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 configured to prevent the detection of lessor secured medical devices or devices with access to medical networks. 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, Office of Information and Technology (OIT) did not manage the configuration and security of certain devices in accordance with VA policy.

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.

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 monitored for compliance 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. VA is working towards implementing automated mechanisms to monitor baseline compliance on all platforms. By not implementing consistent agency-wide configuration management standards for major applications and general support systems, VA is placing critical systems at unnecessary risk of unauthorized access, alteration, or destruction.

CORRECTIVE ACTIONS RECOMMENDED

11. We recommended the 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.)*
12. 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.)*
13. 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 monitored for compliance with established VA security standards. *(This is a repeat recommendation from prior years.)*

14. 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 repeat recommendation from prior years.)*
15. 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.)*
16. 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 partially concurred with recommendations 11 and 12; concurred with recommendations 13, 14, and 16; and non-concurred with recommendation 15. For all the recommendations, the Assistant Secretary stated additional details regarding activities to address the identified findings have been provided to the OIG contracted auditors.

OIG Response

The Assistant Secretary for Information and Technology's planned corrective actions are responsive to recommendations 11, 12, 13, 14, and 16.² While the Assistant Secretary partially concurred with recommendations 11 and 12, OIT's response identified ongoing efforts to address the findings. Regarding the non-concurrence with recommendation 15, the OIG continues to identify vulnerabilities on systems and devices that are not managed by local OIT personnel such as applications or Enterprise Program Management Office systems as stated in the finding above. Accordingly, we stand by our recommendation. The OIG will evaluate applicable compensating controls and determine whether the recommendation can be closed in fiscal year 2022. 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.

² Detailed activities to address the identified findings were provided to the Inspector General. The OIG removed information that is considered sensitive prior to publication.

FISMA Section 3544 requires each agency to establish policies and procedures to ensure information security is addressed throughout the life cycle of each agency information system. The VA Change Management and Knowledge Service policy 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 enforced 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 and several other applications in VA's system inventory. 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

17. We recommended the Acting 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 17 and reported additional details regarding activities to address the identified finding have been provided to the OIG contracted auditors.

OIG Response

The Assistant Secretary for Information and Technology's planned corrective actions are responsive to recommendation 17.³ 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 contingency plans did not always include all required information and were inconsistently documented and tested for the systems and applications that were reviewed during the year. The VA Knowledge Service establishes

³ Detailed activities to address the identified findings were provided to the Inspector General. The OIG removed information that is considered sensitive prior to publication.

high-level policy and procedures for contingency planning and plan testing. Our audit identified the following deficiencies related to contingency planning:

- We 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 were not consistently tested in accordance with VA policy requirements.
- Plans did not consistently document recovery priorities, objectives, or procedures and did not consider dependencies on other related information systems and plans such as supporting infrastructure.

VA established standard recovery goals and procedures for their system boundaries, which makes it difficult to monitor if system specific requirements are being met. 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

18. 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 can be measured and met. *(This is a modified repeat recommendation from prior years.)*
19. We recommended the Assistant Secretary for Information and Technology ensure that contingency plans for all systems are updated to include critical inventory components and are tested in accordance with VA requirements. *(This is a repeat recommendation from prior years.)*

Management Comments

The Assistant Secretary for Information and Technology concurred with recommendations 18 and 19. For the recommendations, the Assistant Secretary reported additional details regarding activities to address the identified findings have been provided to the OIG contracted auditors.

OIG Response

The Assistant Secretary for Information and Technology's planned corrective actions are responsive to recommendations 18 and 19.⁴ 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.

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 monitoring of network segments and tracking and reporting of security events.

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. For instance, 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.

⁴ Detailed activities to address the identified findings were provided to the Inspector General. The OIG removed information that is considered sensitive prior to publication.

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. In prior years, we performed 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. Due to the restrictions associated with the pandemic, we did not perform unannounced scans during FY 2021.

Security Event Tracking and Reporting

Throughout the year, we identified instances of security events that were not reported as incident tickets within the timeframes required by the VA Knowledge Service. 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

20. 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.)*
21. 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.)*
22. 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 20, 21, and 22. For the recommendations, the Assistant Secretary stated additional details regarding activities to address the identified findings have been provided to the OIG contracted auditors.

OIG Response

The Assistant Secretary for Information and Technology's planned corrective actions are responsive to recommendations 20, 21, and 22.⁵ OIT's response identified ongoing efforts to address the finding. 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 an effective patch and vulnerability management process to all devices across the enterprise. In addition, an effective agency-wide process was not fully implemented for using automation to identify and remove prohibited 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.

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 controls that were not addressed during assessments. 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.

⁵ Detailed activities to address the identified findings were provided to the Inspector General. The OIG removed information that is considered sensitive prior to publication.

Due to inadequate monitoring procedures, our 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 its networks, VA is at risk that 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.

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

23. We recommended the Assistant Secretary for Information and Technology implement improved measures to ensure that all security controls are assessed in accordance with VA policy and that identified issues or weaknesses are adequately documented and tracked within POA&Ms. (*This is a repeat recommendation from prior years.*)
24. 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.)*

25. 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 23, 24, and 25. For the recommendations, the Assistant Secretary stated additional details regarding activities to address the identified findings have been provided to the OIG contracted auditors.

OIG Response

The Assistant Secretary for Information and Technology's planned corrective actions are responsive to recommendations 23, 24, and 25.⁶ 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, the VA Knowledge Service 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 2021. 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 appropriate 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 and operated systems such as HR Smart, My HealtheVet, Long Term Solutions, Community Care Referrals and Authorizations, and the VA Time and Attendance System.

⁶ Detailed activities to address the identified findings were provided to the Inspector General. The OIG removed information that is considered sensitive prior to publication.

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

CORRECTIVE ACTIONS RECOMMENDED

26. We recommended the 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 repeat recommendation from prior years.*)

Management Comments

The Assistant Secretary for Information and Technology non-concurred with recommendation 26. The Assistant Secretary stated that their response was pending additional information from the OIG.

OIG Response

Regarding the Assistant Secretary's non-concurrence with recommendation 26, the OIG met with OIT management in February 2022 after issuing the draft report in January to discuss this recommendation. The OIG provided additional information related to this finding and recommendation. The OIG does not believe any additional pending information requests are outstanding. The OIG's testing continues to identify security deficiencies related to internal controls operating on third party managed systems as well as weaknesses with the overall monitoring of the security documentation and practices of those services Accordingly, we stand by our recommendation. The OIG will evaluate applicable controls and determine whether the recommendation can be closed in fiscal year 2022. 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 prior year recommendations. All prior year recommendations are repeated or modified and remain open within the body of this report.

Appendix B: Background

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

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

OMB and DHS provide instructions to Federal agencies and Inspectors General for preparing annual FISMA reports. In November 2020, OMB issued Memorandum M-21-02, *Fiscal Year 2020-2021 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 2021 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, supply chain 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 2021. 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 50 selected major applications and general support systems hosted at 24 VA facilities and on the VA Enterprise Cloud 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 2021 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:

- VA Medical Facility—Albany
- Information Technology Center—Austin
- VA Medical Facility—Columbia
- VA Regional Office—Columbia
- VA Medical Facility—Dayton
- VA Medical Facility—Des Moines
- VA Regional Office—Des Moines
- VA Medical Facility—Hampton
- Information Technology Center—Hines
- VA Medical Facility—Lexington
- VA Medical Facility—Little Rock
- VA Medical Facility—Loma Linda
- Cyber Security Operations Center—Martinsburg

- Capital Region Readiness Center—Martinsburg
- Information Technology Center—Philadelphia
- VA Regional Office—Philadelphia
- VA Medical Facility—Philadelphia
- Vendor Resource Management—Plano
- National Cemetery Administration—Quantico
- VA Medical Facility—Reno
- VA Regional Office—Reno
- VA Medical Facility—Salt Lake City
- VA Medical Facility—South Texas
- VA Enterprise Cloud—Virtual
- VA Medical Facility—Washington DC

We evaluated 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. The testing this year was conducted remotely or virtually where feasible due to the restrictions in place surrounding the Covid-19 pandemic.

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 15, 2022

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

Subj: Draft OIG Report: VA's Federal Information Security Management Act (FISMA) Audit for Fiscal Year 2021 Project Number 2021-01309-AE-0057 (VIEWS 06752047)

To: Assistant Inspector General for Audits and Evaluations

1. The Office of Information and Technology (OIT) is responding to the Office of Inspector General (OIG) Draft Report, Federal Information Security Modernization Act Audit for Fiscal Year 2021 (FISMA).
2. CliftonLarsonAllen LLP is responsible for the findings and recommendations included in the report. Accordingly, the OIG does not express an opinion on VA's information security program in place during FY 2021. CliftonLarsonAllen LLP will follow up on the outstanding recommendations and evaluate the adequacy of corrective actions during its FY 2022 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.
3. The FISMA report provides 26 recommendations for improving VA's information security program. The FY 2020 FISMA report also provided 26 recommendations for improvement. Some recommendations were modified or not closed because relevant information security control deficiencies identified during the FY 2021 FISMA audit were repeat deficiencies. Despite VA's commitment to close the recommendations, some of them have been repeated for multiple years.
4. OIT submits written comments to the recommendations and provided a target implementation date and supporting evidence for each recommendation as appropriate.

The OIG removed point of contact information prior to publication.

(Original signed by)

Kurt D. DelBene

Attachment

Office of Information and Technology

Comments on OIG Draft Report,

“Federal Information Security Modernization Act Audit for Fiscal Year 2021”

The OIG removed information that is sensitive prior to publication. All responses in brackets are included to denote sensitive information from OIT.

Recommendation 1: The OIG recommends 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 repeat recommendation from prior years.)

OIT Response: VA concurs with this recommendation. Within the next 3 months, The Department of Veterans Affairs (VA) Office of Information Security (OIS) will expand the number of systems undergoing the additional Step 4 Control Review risk mitigation activity and iteratively address lessons learned to refine the process. The number of systems undergoing Step 4 Control Reviews has increased from Fiscal Year 2021 (FY21) to encompass a broader scope of systems, including Financially Relevant Systems and High Value Assets.

Within the next 6 months, OIS will implement the developed Governance, Risk, and Compliance (GRC) annual self-assessment review for stakeholder validation to document test evidence and implement accountability structure for approvals. Furthermore, Step 4 Control Reviews will continue to iteratively refine control review methodologies to address high risk control areas. [Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).]

Target Completion Date: Estimated completion by September 2023.

Recommendation 2: The OIG recommends the Assistant Secretary for Information and Technology implement improved mechanisms to ensure system stewards and updating Plans of Action and Milestones for all known risks and weaknesses including those identified during security control assessments. (This is a repeat recommendation from prior years.)

OIT Response: VA concurs with this recommendation. Within the next 3 months, Office of Information Technology (OIT) will continue to hold updated GRC tool trainings that support end users' responsibility and understanding of Plan of Action and Milestone (POAM) processes, providing hands-on demonstrations of required processes in the tool. Authorizing Official Designated Representatives (AODR) are developing processes to include metrics to enable quantitative risk reviews for Area Boundaries and POAMs; if the control compliance status does not mirror open POAMs, then the package is returned for rework.

Within the next 6 months, OIS will leverage Step 4 Control Reviews and Integrated Audit Readiness capabilities for proactive sampling of sites to determine POAM compliance and audit readiness procedures. Additionally, VA plans to implement its accountability structure for system stakeholders, which includes enforcing Authorizing Officials' (AO's) role in evaluating Risk Reviews and understanding the severity of control weaknesses. [Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).]

Target Completion Date: Estimated completion by September 2022.

Recommendation 3: The OIG recommends 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 repeat recommendation from prior years.)

OIT Response: VA partially concurs with this recommendation. VA concurs that system stakeholders are not following the prescribed procedure for obtaining appropriate documentation prior to closing Plans of Action and Milestones, however, mitigating controls are in place that reduce the risk when documentation is not initially closing POAMs appropriately. VA System Owners are responsible for documenting POAMs within the GRC tool where VA has established workflows. These workflows that have been put in place require System Owners to upload applicable documentation, which then prompts a review by the Information Systems Security Officer (ISSO), as documented via the POAM Management Guide, before they can close the POAM within the tool. There is currently a process in place for the closure of POAMs, as well as established roles and responsibilities throughout the process detailing necessary activities. [Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).]

Target Completion Date: Estimated completion by September 2022.

Recommendation 4: The OIG recommends 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. Although there are procedural controls requiring implementation details, OIS is working on a technical solution to ensure implementation details be populated prior to submission of an SSP.

Target Completion Date: Estimated completion by September 2023.

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

OIT Response: VA concurs with this recommendation. Within the next 9 months, OIT will finalize accountability measures for stakeholders to perform quantitative reviews on key security documentation to remain compliant with VA policy.

Target Completion Date: Estimated completion by December 2022.

Recommendation 6: The OIG recommends 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. [Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).]

Target Completion Date: Estimated completion by December 2024.

Recommendation 7: The OIG recommends 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: Estimated completion by December 2024.

Recommendation 8: The OIG recommends 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: Estimated completion by December 2022.

Recommendation 9: The OIG recommends the Office of Personnel Security, Human Resources, and Contract Offices implement improved processes for establishing and maintaining accurate data within VA's authoritative system of record for background investigations. (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: Estimated completion by June 2023.

Recommendation 10: The OIG recommends the Office of Personnel Security, Human Resources, and Contract Offices strengthen processes to ensure appropriate levels of background investigations are completed for applicable VA employees and contractors. (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: Estimated completion by June 2023.

Recommendation 11: The OIG recommends 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 partially concurs with this recommendation. [Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).]

Target Completion Date: Estimated completion by September 2023.

Recommendation 12: The OIG recommends 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 partially concurs with this recommendation. [Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).]

Target Completion Date: Estimated completion by September 2023.

Recommendation 13: The OIG recommends the Assistant Secretary for Information and Technology maintain a complete and accurate security baseline configuration for all platforms and ensure all baselines are appropriately monitored 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: Estimated completion by November 2023.

Recommendation 14: The OIG recommends 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 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: Estimated completion by March 2022.

Recommendation 15: The OIG recommends 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 does not concur with this recommendation. [Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG).]

Target Completion Date: VA requests closure to this recommendation

Recommendation 16: The OIG recommends 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: Estimated completion by December 2023.

Recommendation 17: The OIG recommends 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: Estimated completion by September 2024.

Recommendation 18: The OIG recommends 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 can be measured and 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: Completed. VA requests closure since evidence has been provided.

Recommendation 19: The OIG recommends the Assistant Secretary for Information and Technology ensure that contingency plans for all systems are updated to include critical inventory components and are tested in accordance with VA requirements. (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: Completed. VA requests closure since evidence has been provided.

Recommendation 20: The OIG recommends 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: Completed. VA requests closure since evidence has been provided.

Recommendation 21: The OIG recommends 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: Estimated completion date by December 2022.

Recommendation 22: The OIG recommends 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).]

Recommendation 23: The OIG recommends the Assistant Secretary for Information and Technology implement improved measures to ensure that all security controls are assessed in accordance with VA policy and that identified issues or weaknesses are adequately documented and tracked within POA&Ms. (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: Estimated completion date by September 2023.

Recommendation 24: The OIG recommends 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: Estimated completion date by December 2022.

Recommendation 25: The OIG recommends 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: Estimated completion date by November 2022.

Recommendation 26: The OIG recommends 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 repeat recommendation from prior years.)

OIT Response: VA non-concurs with this recommendation. Response pending additional information from the OIG.

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 Benefits Administration
Veterans Health 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
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget
Department of Homeland Security

OIG reports are available at www.va.gov/oig.