US 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 2024

Audit	24-01233-90	June 18, 2025

BE A
VOICE FOR
VETERANS
REPORT WRONGDOING
vaoig.gov/hotline | 800.488.8244

OUR MISSION

To serve veterans and the public by conducting meaningful independent oversight of the Department of Veterans Affairs.

CONNECT WITH US

Subscribe to receive updates on reports, press releases, congressional testimony, and more. Follow us at @VetAffairsOIG.

PRIVACY NOTICE

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.

MEMORANDUM

TO: Assistant Secretary for Information and Technology and Chief Information Officer

FROM: Larry Reinkemeyer, Assistant Inspector General, Office of Audits and Evaluations, VA Office of Inspector General

SUBJECT: Federal Information Security Modernization Act (FISMA) Audit for Fiscal Year (FY) 2024

1. Enclosed is the final report, *Federal Information Security Modernization Act Audit for Fiscal Year 2024*. The VA Office of Inspector General (OIG) contracted with the independent public accounting firm CliftonLarsonAllen LLP (CLA) 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 annually review 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. CLA is responsible for the findings and recommendations included in this report. Accordingly, the OIG does not express an opinion on the information security program VA had in place during FY 2024. CLA will follow up on open recommendations and evaluate the adequacy of corrective actions during its FY 2025 FISMA audit. According to CLA's findings, 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
    - address security-related issues that contributed to the information technology material weakness reported in the FY 2024 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 facilities; and
    - improve performance monitoring to ensure controls are operating as intended for all systems and communicate identified security deficiencies to the appropriate personnel so they can mitigate significant security risks.

4. This report provides 23 recommendations for improving VA's information security program. The FY 2023 FISMA report provided 25 recommendations for improvement. Some recommendations were modified or not closed because relevant information security control deficiencies identified during the FY 2024 FISMA audit were repeat deficiencies. Two prior-year recommendations were closed because VA improved how it monitors controls for contractor systems and detects unauthorized vulnerability scans. Two recommendations were removed as stand-alone items and merged with an existing recommendation to avoid duplication. Two new recommendations were added to the report. Despite VA's commitment to complete the actions needed to close the recommendations, some recommendations have been repeated for multiple years.
5. The effect of the open recommendations will be considered in the FY 2025 audit of VA's information security program. The OIG remains concerned that continuing delays in addressing these open recommendations could contribute to reporting a material weakness in VA's information technology security controls during the FY 2025 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

June 3, 2025
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) ending September 30, 2024. 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 (SP) 800-53, Revision 5, Security and Privacy Controls for 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 49 selected major applications and general support systems hosted at 23 VA facilities and 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 2024 through October 2024.

Based on our audit procedures, we concluded that VA continues to face significant challenges meeting the requirements of FISMA. This report provides 23 recommendations to assist VA in strengthening its information security program.

In connection with the audit of VA's FY 2024 Consolidated Financial Statements, we evaluated general computer and application controls for VA's major financial management systems. Significant deficiencies identified during our 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 July 2024. 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 30, 2024. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to October 30, 2024. 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

Arlington, Virginia
June 3, 2025

Table of 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 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 2024 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 23 VA facilities and the VA Enterprise Cloud. In FY 2024, we identified specific deficiencies in the following areas:

1. Agency-Wide Security Management Program
2. Background Investigations
3. Contingency Planning
4. Identity Management and Access Controls
5. Configuration Management
6. Incident Response and Monitoring
7. Vulnerability Management

This report provides 23 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 2024 FISMA audit were repeat deficiencies. Two prior year recommendations were closed because VA has made improvements in the monitoring of controls for contractor systems and detection of unauthorized vulnerability scans. Two recommendations were removed as stand-alone items and merged with existing recommendations to avoid any duplication. Two new recommendations were added to the report. Appendix A provides more details regarding the closed recommendations. The FY 2023 FISMA report provided 25 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 and risk management program to meet FISMA requirements. Consequently, this audit identified continuing deficiencies related to access controls, configuration management controls, security 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 2024, VA's Chief Information Officer continued the Enterprise Cybersecurity Strategy Program (ECSP) to implement the VA Cybersecurity Strategy (VA issued a new cybersecurity strategy in FY 2022). Several initiatives were launched, new tools were 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 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 Information Technology material weakness reported as part of the Consolidated Financial Statement Audit. As part of the ongoing ECSP efforts, we noted improvements related to:

- Increase in visibility to infrastructure platforms and host-based protection solutions.
- Continued maturation of processes related to developing and maintaining assessment and authorization documentation within the Governance, Risk, and Compliance tool.
- Improvement in the remediation of aged vulnerabilities on network devices and components.

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 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.

Risk Management

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, control assessments, Plans of Action and Milestones (POA&Ms), and

Authority to Operate processes, and system security plans. Each of these processes is essential for protecting VA's mission-critical systems through appropriate risk mitigation strategies.

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, we identified several instances of systems where Risk Assessments, Control Responses, and Privacy Impact Assessments were not documented or updated in accordance with VA standards.

Inconsistent Security Control Assessments and System Security Plans

VA has incorporated security control assessments within its continuous monitoring program to monitor and manage system security controls. However, we noted that assessments were not performed by independent groups and certain system security deficiencies were not incorporated into POA&M management and risk management activities. The group that performs the independent assessments was only able to assess a small portion of the systems that go through Authorization reviews during a given year. We also identified numerous instances of system security plans where controls were not assessed, documented with generic non-descriptive responses, or inappropriately marked as not applicable.

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.

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 22,248 ongoing POA&M items in FY 2024, as compared with 26,197 open POA&Ms in FY 2023. 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.

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. 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.

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, regarding the independent evaluation of 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 processes for reviewing and updating key security documentation, including Security Control Assessments, Risk Assessments, and Privacy Impact Assessments as needed. Such updates will ensure all required information is included and accurately reflects the current environment, new security risks, and applicable Federal standards. *(This is a modified repeat recommendation from prior years.)*
3. We recommended the Assistant Secretary for Information and Technology implement improved processes to ensure System Security Plans reflect the status of security control implementations and risks are accurately reported to support a comprehensive risk management program across the organization. *(This is a modified repeat recommendation from prior years.)*
4. We recommended the Assistant Secretary for Information and Technology implement improved mechanisms to ensure system owners and information system security officers follow procedures for establishing, tracking, and updating POA&Ms for all known risks and weaknesses including those identified during security control and other assessments. *(This is a repeat recommendation from prior years.)*
5. We recommended the Assistant Secretary for Information and Technology implement measures to ensure that system stewards and other officials responsible for system level POA&Ms are closing items with relevant support that shows sufficient remediation of the identified weakness. *(This is a modified repeat recommendation from prior years.)*

Management Comments

The acting Assistant Secretary for Information and Technology concurred with recommendations 1, 2, and 3 but did not concur with recommendations 4 and 5. For recommendations 1, 2, and 3, the acting Assistant Secretary reported that VA's risk-based approach to continuous monitoring and independent security control assessments has effectively identified and mitigated potential risks to VA's mission-critical systems. By prioritizing security control assessments against critical systems and high-value assets, VA has made sure controls are implemented and control weaknesses reported accurately, reducing the risk of security incidents. Additionally, the acting Assistant Secretary stated VA's continuous monitoring program has achieved significant milestones, including (1) deploying a near real-time capability and process with visibility into key security documentation for security updates to include security control assessments, risk assessments, and privacy impact assessments, as needed, enabling VA to proactively identify and address potential vulnerabilities; and (2) enhanced role-based training for system security personnel, which improved key security control documentation. For VA's non-concurrence with recommendations 4 and 5, the acting Assistant Secretary reported 99 percent of identified POA&M closures contained all appropriate documentation to close the findings, and this "risk-based approach to POA&M management is successfully identifying and addressing potential vulnerabilities." Additionally, he reported VA reduced 90 percent of ongoing POA&Ms older than three years, "demonstrating VA's ability to prioritize and address high-risk vulnerabilities in a timely manner."

OIG Contractor Response

The acting Assistant Secretary for Information and Technology's planned corrective actions are responsive to recommendations 1, 2, and 3. The OIG designated contractor will monitor VA's progress and follow up on implementation of the recommendations until all proposed actions are completed. Regarding recommendations 4 and 5, Plans of Action and Milestones testing was performed on 48 VA systems. For 2 of the systems tested, we identified instances where Plans of Action and Milestones were not consistently documented with the required elements such as impact, mitigations, and recommendations. In addition, we identified several Plans of Action and Milestones that were closed with inappropriate or insufficient support to justify the remediation of the original security risk. Our testing was based on samples of closed Plans of Action and Milestones for each system and did not demonstrate a 99 percent compliance rate; contrary to management assertions. Furthermore, without sufficient documentation to justify closure of Plans of Action and Milestones, VA cannot ensure that system security risks have been fully mitigated. Accordingly, we stand by recommendations 4 and 5 that VA's processes for Plans of Action and Milestones need improvement to ensure that corrective actions are comprehensively tracked and updated to reflect their current status. The OIG designated contractor 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.

Background Investigations

The completion and favorable adjudication of a background investigation, at the designated level based on a position's Risk and Sensitivity, is required for all VA personnel and contractors. Access to VA information and systems can be granted with a favorably adjudicated fingerprint which is a required first step in the background investigation process. Background investigations and the underlying processes for them were reviewed from an enterprise perspective and at 13 of 23 sites within our audit scope. Issues were noted related to establishing the appropriate level of background investigations and performing reinvestigations timely. VA informed us that they have begun enrolling individuals in continuous vetting which removes the requirement for reinvestigations but this process was ongoing during the period. Without accurate and standardized methods for establishing and tracking employee investigation data across the enterprise, the VA is at risk of allowing individuals to access sensitive data and systems with outdated or inappropriate levels of investigation.

CORRECTIVE ACTIONS RECOMMENDED

6. We recommended the VA Office of Personnel Security, Human Resources, and Contract Offices strengthen processes to ensure appropriate levels of background investigations are performed timely and completed for applicable VA employees and contractors. *(This is a repeat recommendation from prior years.)*
7. We recommended the Office of Personnel Security, Human Resources, and Contract Offices implement improved processes for establishing and maintaining accurate investigation data within VA systems used for background investigations. *(This is a repeat recommendation from prior years.)*

Management Comments

The acting Assistant Secretary for Information and Technology concurred with recommendations 6 and 7. For those recommendations, the acting Assistant Secretary reported that VA's Centralized Adjudication Background Investigation System (VA-CABS) has "significantly" increased VA's risk management and mitigation related to background investigations and adjudications. He said the integration of VA-CABS 2.0 with HR-Smart and Account Provisioning and De-provisioning System is meant to improve accuracy and consistency of position designation data to make sure employees and contractors get background investigations at the appropriate level.

OIG Contractor Response

The acting Assistant Secretary for Information and Technology's planned corrective actions are responsive to recommendations 6 and 7. The OIG designated contractor 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.

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

- Information system contingency plans were not consistently tested in accordance with VA policy requirements.
- We identified several instances of system disruptions and outages related to the primary VA health record application that were not resolved within documented recovery time objectives.

Inconsistent documentation and testing of system contingency plans could increase the risk that VA sensitive data and business functions could become unavailable and adversely impact business operations in the event of a system disruption. In addition, without monitoring performance of real-world system events to their associated boundaries, VA is at risk of not consistently meeting recovery objectives when restoring systems in response to a disaster or disruption.

CORRECTIVE ACTIONS RECOMMENDED

8. We recommended the Assistant Secretary for Information and Technology ensure contingency plans for all systems and applications are updated and tested in accordance with VA requirements. *(This is a repeat recommendation from prior years.)*
9. We recommended the Assistant Secretary for Information and Technology implement improved procedures to ensure that system outages are resolved within stated recovery time objectives. *(This is a modified repeat recommendation from prior years.)*

Management Comments

The acting Assistant Secretary for Information and Technology concurred with recommendations 8 and 9. For those recommendations, the acting Assistant Secretary reported VA continues to improve contingency planning with standardized templates, training, and monitoring testing performance to reduce operational risk. He reported recent achievements such as updates to contingency planning handbook, contingency planning controls, standard operating procedures, and control correlation identifiers to comply with the National Institute of Standards and Technology and federal guidance; action items for all VA systems to review, update, and test information system contingency plans and disaster recovery plans to promote preparedness and risk awareness; and a training program focused on testing and operations to help with responses to disruptions and ensure critical services continuity.

OIG Contractor Response

The acting Assistant Secretary for Information and Technology's planned corrective actions are responsive to recommendations 8 and 9. The OIG designated contractor 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 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 account reviews, access management, and password management. Access control testing was performed at all sites and for all systems in scope of our review. For access controls to be effective, VA needs to have improved collaboration amongst all stakeholders and system owners since there is no single point of accountability within its highly decentralized computer environment.

Account Reviews

Our assessment identified several instances of VA systems and applications where there were insufficient procedures related to the periodic review of end user and privileged account access rights. These reviews are critical to ensure that end users and system accounts only have access to the data and processes they need to perform their job functions. The VA Knowledge Service details high level requirements related to the process for reviewing of system and application accounts, however, these processes can be labor intensive to implement and operate and often require coordination and involvement from business units or other organizations outside of IT.

Access Management

We also noted several instances of inadequate documentation of approvals for system access, excessive access permissions, as well as a large number of users who did not have their accounts disabled in a timely manner after separation. The VA Knowledge Service details access management policies and procedures for VA's information systems. However, due to the size of the user base for VA systems and the fluid nature of the staffing environment these processes can be difficult to manage across the entire portfolio of VA applications. Maintenance of access approvals and the timely disablement of accounts when no longer needed are critical controls for ensuring only authorized users have access to VA systems and data.

Password Management

The audit team continued to identify multiple instances of VA systems and applications where there were service accounts that had not had passwords changed in over 3 years in accordance with policy. Additionally, many systems did not have controls in place to periodically review service accounts for continued need and appropriateness. Lack of control of service accounts increases the risk of unauthorized access, loss, or compromise of VA sensitive data. We also identified numerous authentication and weak password issues during vulnerability scans of VA applications and networks.

CORRECTIVE ACTION RECOMMENDED

10. We recommended the Assistant Secretary for Information and Technology ensure system owners consistently implement processes for periodic reviews of user account access. Remove unnecessary and inactive accounts on systems and networks. *(This is a modified repeat recommendation from prior years.)*

11. We recommended the Assistant Secretary for Information and Technology coordinate with system owners and local system management to ensure the consistent monitoring and reviewing of privileged accounts, service accounts, and accounts for individuals with access to source code repositories are performed across VA systems and platforms. *(This is a new recommendation.)*

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

Management Comments

The acting Assistant Secretary for Information and Technology did not concur with recommendations 10, 11, and 12. For recommendations 10 and 11, he reported VA has achieved "a significant level of maturity" related to access management practices, including the following data on reviewed systems: 72 percent had no findings related to user access reviews; 86 percent had no findings related to disabling inactive user accounts; 94 percent had no findings related to user access approvals or evidence of approvals; and 82 percent had no findings related to approvals for privileged access. Concerning recommendation 12, VA is "ensuring that all published VA enterprise secure configuration checklists/platform baselines have assessment strategies that are properly documented and configured to use enterprise automated monitoring tools where possible, enabling us [VA] to identify and remediate potential security vulnerabilities in a timely manner."

OIG Contractor Response

Regarding recommendations 10, 11, and 12, independent access control testing was performed at all sites evaluated during the FY 24 audit. For access controls to be effective, VA needs to have improved collaboration amongst all stakeholders and system owners since there is no single point of accountability within its highly decentralized computer environment. Additionally, we noted significant issues related to controls for account management on several systems that were tested during the year. For many VA system and application boundaries, we noted inconsistent reviews of user access resulting in numerous systems, terminated, and inactive user accounts that were not removed from the applications and networks. In addition, inconsistent exit clearance processes for employees contributed to a significant number of accounts that were not disabled timely. Further, proper completion of user access requests was not consistently performed to eliminate conflicting roles and enforce principles of least system privilege. Finally, we identified numerous service accounts that were not needed or had passwords that were not changed in

over three years in accordance with VA policy. These service accounts supported various systems, such as databases, mainframe systems supporting financial applications. Accordingly, we stand by recommendations 10, 11, and 12 that VA's system access controls need improvement to minimize the risk of unauthorized system access and the lack of accountability for actions performed. Furthermore, consistent user account reviews are critical to restrict legitimate users to specific systems, programs, and data in order to prevent unauthorized access. Without appropriate technical access controls, there is an increased risk that users will be granted inappropriate and excessive systems privileges. The OIG designated contractor 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

Configuration Management testing was performed at the enterprise level and for 49 selected system, application, and geographic "area" boundaries. We noted issues related to the implementation of change management policy, implementation and monitoring of baseline configurations, implementation of an accurate system and component inventory, and the monitoring for changes to system settings and software.

Change Management

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 that did not follow standardized software change control procedures.

FISMA Section 3554 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.

We also identified several VA systems and applications where there were insufficient controls in place for reviewing system changes to ensure that only authorized modifications were implemented. Without consistent change control and review procedures in place VA is at risk of allowing unauthorized or insufficiently tested modifications to their critical systems and data.

Baseline Security Configurations

VA developed guidelines to define agency-wide security configuration baselines for its major information system components. FISMA Section 3554 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 devices that were not configured to a common security configuration standard, resulting in misconfigurations or non-compliance with VA configuration baselines. VA's large and federated systems environment makes it difficult to consistently implement and enforce configuration standards. 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.

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 compile an inventory of network components that support critical applications and program 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.

In addition, an effective agency-wide process was not fully implemented for using automation to identify or prevent unauthorized changes 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 5, Security and Privacy Controls for Information Systems and Organizations, outlines the importance of deploying automated mechanisms to detect unauthorized components and configurations within agency networks.

CORRECTIVE ACTIONS RECOMMENDED

13. We recommended the Assistant Secretary for Information and Technology ensure established change control procedures are consistently followed for testing and approval of system changes for VA applications and networks. *(This is a modified repeat recommendation from prior years.)*
14. We recommended the Assistant Secretary for Information and Technology implement and consistently enforce established procedures for preventing and detecting potential unauthorized changes across all platforms and applications in the environment. *(This is a modified repeat recommendation from prior years.)*
15. We recommended the Assistant Secretary for Information and Technology ensure that all systems and platforms are monitored for compliance with documented VA standards for baseline configurations. Ensure that system owners consistently implement and monitor their configurations. *(This is a modified repeat recommendation from prior years.)*
16. We recommended the Assistant Secretary for Information and Technology implement automated software management processes on all agency platforms to identify and prevent the use of unauthorized software on agency devices. *(This is a new recommendation.)*
17. We recommended the Assistant Secretary for Information and Technology implement improved procedures for establishing, documenting, and monitoring an accurate software and

logical hardware inventory for system boundaries across the enterprise. *(This is a modified repeat recommendation from prior years.)*

Management Comments

The acting Assistant Secretary for Information and Technology concurred with recommendations 13, 14, and 15 but did not concur with recommendations 16 and 17. For recommendations 13 and 14, the acting Assistant Secretary reported that VA continues to improve "change control processes to demonstrate effectiveness in managing and mitigating risks associated with changes to VA's information technology systems" and that the policy on the process clearly guides implementation. For recommendation 15, the acting Assistant Secretary stated that VA also continues to improve efforts to establish and maintain secure configuration settings to make sure "all systems are configured to meet established security standards." For VA's non-concurrences with recommendations 16 and 17, the acting Assistant Secretary stated that VA's application monitoring process and application control initiative have mitigated unauthorized software usage risks; further, VA's logical hardware inventory processes have been effective at mitigating hardware inventory management risks. In addition to a standard operating procedure the acting Assistant Secretary said has improved compliance and accuracy identifying connected hardware, VA is also "in the final stages of transitioning to a comprehensive framework, enterprise Software Asset Management program, that will deploy end-to-end accountability and security measures for software that will further mature software asset management."

OIG Contractor Response

The acting Assistant Secretary for Information and Technology's planned corrective actions are responsive to recommendations 13, 14, and 15. The OIG designated contractor will monitor VA's progress and follow up on implementation of the recommendations until all proposed actions are completed. Regarding the non-concurrences with recommendations 16 and 17, configuration management testing was performed at the enterprise level and for 49 selected systems, applications, and geographic "area" boundaries. We noted several issues related to the implementation of change management policy, implementation and monitoring of baseline configurations, implementation of an accurate system and component inventory, and the monitoring for changes to system settings and software. Specifically, we noted that VA did not enforce a "deny-all, permit-by-exception" (Whitelist) policy to prevent the installation of unauthorized software programs on its "High and Moderate Impact" information systems. Additionally, some mission critical systems were not covered under an automated software management process to identify and remove prohibited software. Moreover, we observed that VA is still in the process of establishing a comprehensive software inventory to track usage across the enterprise and VA does not have an accurate tracking of mission critical components and applications within the VA system boundary. Accordingly, we stand by recommendations 16 and 17 that VA's automated software management and software/hardware inventory processes need improvement to minimize the risk that dangerous malware will not be introduced into the computing environment. The lack of accurate logical system inventory increases the risk of improper component management, as well as an increased risk of improper component accountability. The OIG designated contractor 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

VA has implemented several Security Incident and Event Management tools 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, we noted several instances of major applications where audit logs were not consistently reviewed or monitored. VA did not consistently ensure that non-common platforms and application layer audit logs were collected and reviewed for the purpose of ongoing monitoring. Without adequate coverage of log review processes and 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.

Audit Log Review

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 effectively managed, aggregated, or proactively reviewed for significant systems such as the Financial Management System. 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.

CORRECTIVE ACTIONS RECOMMENDED

18. We recommended the Assistant Secretary for Information and Technology implement improved processes for monitoring and analyzing significant system audit events for unauthorized or unusual activities across all systems and platforms in accordance with VA policy. Ensure privileged activity is monitored on all systems and applications. *(This is a modified repeat recommendation from prior years.)*
19. 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.)*

Management Comments

The acting Assistant Secretary for Information and Technology concurred with recommendations 18 and 19. The acting Assistant Secretary reported that "VA continues to drive maturity in our ongoing efforts to enhance incident response and logging capabilities that will significantly improve our ability to detect, respond to, and mitigate cybersecurity threats." The acting Assistant Secretary said VA also launched an endpoint detection and response capability to capture data that "will be used to triage and investigate incidents in a timely and effective manner. … [to]

provide us with enhanced visibility into system events and anomalies, allowing us to respond quickly to potential security threats."

OIG Contractor Response

The acting Assistant Secretary for Information and Technology's planned corrective actions are responsive to recommendations 18 and 19. The OIG designated contractor 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.

Vulnerability Management

We continued to identify 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 and system configurations. 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. 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.

Unsecure Web Applications and Services

Tests of web-based applications identified instances 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 process to identify web-based vulnerabilities, such as Structured Query Language injection attacks on major systems, the process for documenting, tracking, and remediation of cross-site scripting and web server misconfiguration vulnerabilities was not yet formalized. Consequently, we continue to identify security vulnerabilities on web applications hosted at local facilities.

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, Revision 1, *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 consistently 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 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 4 *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology,* states an agency's patch and vulnerability management program should be integrated with configuration management to ensure efficiency. VA has not consistently 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 consistently 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. While extensive Access Control Lists are used to filter network communication of the general network and medical devices, we continued to identify instances where medical systems have vulnerabilities and are accessible to devices on the general network. Additionally, we identified several medical devices missing security updates and using operating systems and applications that were no longer supported by the vendor for security remediation. Vulnerable devices which have connectivity to otherwise segmented medical systems can expose the segmented medical devices to significant security risks that could allow malicious users to gain unauthorized access onto mission critical applications. 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.

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, the ownership of certain devices and systems were not clearly defined for the purpose of ongoing continuous monitoring and vulnerability remediation. Consequently, some network components, 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.

CORRECTIVE ACTIONS RECOMMENDED

20. We recommended the Assistant Secretary for Information and Technology implement improved mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and Web application servers in accordance with established policy timeframes. If patches cannot be applied or are unavailable, other protections or mitigations should be documented and implemented to address the specific risks. *(This is a modified repeat recommendation from prior years.)*

21. We recommended the Assistant Secretary for Information and Technology continue to implement improved segmentation controls that restrict vulnerable medical devices from unnecessary access from the general network. *(This is a modified repeat recommendation from prior years.)*

22. We recommended the Assistant Secretary for Information and Technology implement improved processes to require system owners and management to provide adequate credentials to ensure security scans are authenticated to end devices where feasible and the subsequent vulnerabilities are remediated in a timely manner. *(This is a modified repeat recommendation from prior years.)*

23. We recommended the Assistant Secretary for Information and Technology improve the process for tracking and resolving vulnerabilities that cannot be addressed by enterprise processes within policy timeframes. Implement mitigations for identified security deficiencies by applying security patches, system software updates, or configuration changes to reduce applicable security risks. *(This is a modified repeat recommendation from prior years.)*

Management Comments

The acting Assistant Secretary for Information and Technology did not concur with recommendations 20, 21, 22, and 23. Specific to recommendation 21, the acting Assistant Secretary noted VA's medical device protection program "has implemented a comprehensive approach to segmenting and protecting networked medical devices" and listed achievements such as enterprise risk assessments being conducted on all networked medical devices to identify and hone security controls, and segmenting devices from the general network using virtual local area networks and access control lists, enforced through network access control tools. The acting Assistant Secretary noted for the other three recommendations VA's commitment to a vulnerability management program that complies with federal and industry standards. He stated that "the program has consistently demonstrated a high level of effectiveness in managing critical and high vulnerabilities, with a sustained performance of 90% or greater." Recent achievements include the following: (1) remediated 100 percent of systems with Priority 1 vulnerabilities within 14 days; (2) maintained a 90 percent average compliance rating in mitigating all critical vulnerabilities; and (3) aligned 90 percent of assets to system boundaries within the governance, risk, and compliance tool, which ensures evaluation of all assets during the assessment and authorization process.

OIG Contractor Response

Regarding the non-concurrences with recommendations 20, 21, 22, and 23, independent vulnerability testing was performed at all VA operated facilities. During testing, we identified numerous critical and high-risk severity vulnerabilities on networks that were due to unpatched, outdated operating systems and applications, and weak security configurations. Specifically, we noted 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. Moreover, we continued to see older security patch issues and previously identified vulnerabilities persist on the networks. We also noted that network segmentation controls were in place to protect most medical devices; however, we identified several medical devices missing security updates and using operating systems and applications that were no longer supported by the vendor for security remediation. Additionally, VA's vulnerability management program did not ensure that credentialed vulnerability testing is performed on all systems across the enterprise. Thus, VA did not have a complete inventory of existing security vulnerabilities on its networks and its remediation efforts were not effective in addressing all security vulnerabilities on critical systems identified during their scanning processes. Finally, VA did not provide us evidence to demonstrate that: 100 percent of systems across the environment that have priority 1 vulnerabilities have been remediated within 14 days and management has maintained an average of 90 percent compliance rating in addressing all critical vulnerabilities across the environment. Accordingly, we stand by recommendations 20, 21, 22, and 23 that VA's vulnerability management processes need improvement. Without remediating significant security vulnerabilities on all platforms, an attacker may be able to gain unauthorized system access to modify or delete sensitive information; disrupt operations; or launch attacks against other VA systems. The OIG designated contractor 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.

Appendix A: Status of Prior Year Recommendations

We noted 23 of 25 prior-year recommendations are repeated or modified and remain open within the body of this report. As noted in the table below, four recommendations were closed during the FY 2024 FISMA audit.

Table A.1. Closed Prior Year Recommendations

Number	Recommendation	Status	Corrective actions
FISMA-2023-15	We recommended the Assistant Secretary for Information and Technology enhance procedures for tracking security responsibilities for networks, devices, and components not managed by the Office of Information and Technology to ensure vulnerabilities are remediated in a timely manner.	Closed	This recommendation was closed as a standalone item and merged with recommendation 21 in this report to avoid any overlap.
FISMA-2023-21	We recommended the Assistant Secretary for Information and Technology implement improved safeguards to identify and prevent unauthorized vulnerability scans on VA networks.	Closed	Additional monitoring capabilities were established which have allowed VA to produce alerts of unexpected port scan activity on network endpoint devices.
FISMA-2023-22	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.	Closed	This recommendation was closed as a standalone item and merged with modified recommendation 3 in this report to avoid any overlap.

Number	Recommendation	Status	Corrective actions
FISMA-2023-25	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.	Closed	During the FY 2024 audit, we noted improvements in contractor oversight and significantly fewer control deficiencies. We will continue to evaluate contractor systems security control performance in future audit cycles.

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 December 2023, OMB issued Memorandum M-24-04, *Fiscal Year 2024 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.

OMB also selected a core group of metrics, representing a combination of Administration priorities and other highly valuable controls, which must be evaluated annually. The remainder of the standards and controls will be evaluated in metrics on a two-year cycle. For FY 2024, the metrics consisted of the core metrics and FY 2024 supplemental metrics.

The FY 2024 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 2024. 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 23 physical 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 2024 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.

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
- VA Medical Facility – Boise
- VA Medical Facility – Buffalo
- VA Regional Office – Detroit
- VA Medical Facility – Grand Junction
- Information Technology Center – Hines
- VA Medical Facility – Honolulu
- VA Medical Facility – Huntington
- VA Medical Facility – Madison
- Cyber Security Operations Center and Capital Region Readiness Center – Martinsburg
- VA Regional Office – Montgomery
- VA Regional Office – New Jersey
- VA Medical Facility – Northport

- VA Medical Facility – Orlando
- VA Medical Facility – Palo Alto
- Information Technology Center – Philadelphia
- VA Medical Facility - Phoenix
- VA Medical Facility – Portland
- VA Medical Facility – San Diego
- VA Regional Office – Saint Louis
- VA Medical Facility – Salem
- VA Medical Facility – Shreveport
- Loan Guaranty Service – Vendor Resource Management
- VA Enterprise Cloud – Virtual

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.

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: April 9, 2025

From: Deputy Chief Information Officer, Connectivity and Collaboration Services, Performing the Delegable Duties of the Assistant Secretary for Information and Technology and Chief Information Officer (005)

Subj: Office of Inspect General Draft Report, Federal Information Security Modernization Act Audit for Fiscal Year 2024 (VIEWS 12838382)

To: Assistant Inspector General for Audits and Evaluations (52)

1. Thank you for the opportunity to comment on the Office of Inspector General (OIG) draft report, Federal Information Security Modernization Act Audit for Fiscal Year 2024.

2. The report provides 23 recommendations for improving the Department's information security program. The Office of Information and Technology (OIT) is submitting the attached written comments to the recommendations, including strategic responses and accomplishments and remediation goals.

The OIG removed point of contact information prior to publication.

(Original signed by)

Eddie Pool

Attachment

Attachment

Office of Information and Technology

Comments to Office of Inspector General Draft Report,

"Federal Information Security Modernization Act Audit for Fiscal Year 2024"

(VIEWS 12838382)

Fiscal Year (FY) 2024 Federal Information Security Modernization Act (FISMA) Audit Response Summary

Thank you for the opportunity to review the Office of Inspector General (OIG) report, *Federal Information Security Modernization Act Audit for Fiscal Year 2024*. This report provides valuable insights into our organization's security control compliance and highlights the importance of our continued partnership with OIG's security audit team. The collaboration between the Department of Veterans Affairs (VA) and OIG during the audit cycle underscores the Office of Information and Technology's (OIT) commitment to security excellence.

In FY 2024, OIT made significant strides in achieving strategic goals through a risk-based approach to protecting Veteran data and ensuring the confidentiality, integrity, and availability of essential services for Veterans. The control responses and remediation plans outlined in this response are a direct result of OIT's continued focus on risk management, commensurate with cost and impact to VA's mission. OIT will continue to allocate resources to areas that pose the greatest risk to VA systems and data, directly impacting our ability to deliver services to Veterans. As a result of risk-based prioritization, OIT has demonstrated measurable improvements in all areas of VA's cybersecurity posture.

VA made significant progress throughout FY 2024 in strengthening our cybersecurity in the following areas:

- Plan of action and milestones (POA&M) compliance: VA has maintained greater than 90% POA&M compliance.
- Authorizations to operate (ATO): VA achieved an all-time 3-year high for ATOs (149); the achievement is significant because it shows a high level of trust and compliance in VA systems and reduces the frequency of reauthorization and the associated administrative burden.
- High-value asset (HVA) systems: achieved 100% testing compliance for all HVAs. Ensuring that all HVAs are tested for compliance is critical for protecting the most important and sensitive systems within VA.
- Critical and high aged vulnerabilities: remediated 84%, or 2 million, critical and high aged vulnerabilities. This shows a significant effort in reducing the number of exploitable vulnerabilities, which is essential for maintaining the security of VA's information technology infrastructure.
- Continuous monitoring and enforcement of application controls: enabled continuous monitoring and enforcement of application controls, successfully blocking 100% of prohibited applications on VA's network.

While the annual OIG FISMA audit provides valuable insights into compliance with VA's security policies, a comprehensive risk-based assessment would offer a more nuanced understanding of our security posture. By considering the degree of risk posed by identified deficiencies, we can prioritize remediation efforts that maximize risk reduction. Comprehensive risk assessments that consider the likelihood and

impact of a security deficiency, weighed against mitigating controls, would allow us to focus immediate attention on the most critical vulnerabilities. A risk-based approach enables us to optimize resource allocation, ensuring that our remediation efforts are targeted and effective in reducing the overall risk to our enterprise.

VA values the insights the annual OIG FISMA audit provides and is committed to making demonstrable progress in remediating long-standing security deficiencies. To achieve this goal, VA will continue to resolve identified security weaknesses and align its cybersecurity strategies with broader organizational objectives. As part of this effort, OIT has developed practical and measurable targets for FY 2025, which are attached to these written comments.

OIG FISMA Recommendations 1, 2, and 3

Recommendation 1: We recommended the Assistant Secretary for Information and Technology consistently implement an improved continuous monitoring program in accordance with the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF). Specifically, implement an independent security control assessment process to evaluate the effectiveness of security controls prior to granting authorization decisions.

Recommendation 2: We recommended the Assistant Secretary for Information and Technology implement improved processes for reviewing and updating key security documentation, including Security Control Assessments, Risk Assessments, and Privacy Impact Assessments as needed. Such updates will ensure all required information is included and accurately reflects the current environment, new security risks, and applicable federal standards.

Recommendation 3: We recommended the Assistant Secretary for Information and Technology implement improved processes to ensure System Security Plans reflect the status of security control implementations and risks are accurately reported to support a comprehensive risk management program across the organization.

Comments: Concur with recommendations 1, 2, and 3.

Strategic Response and Accomplishments:

VA concurs with OIG's recommendations. VA's risk-based approach to continuous monitoring and independent security control assessments (SCA) has effectively identified and mitigated potential risks to VA's mission critical systems. By prioritizing SCAs against critical systems and HVAs, we have ensured that controls are properly implemented, and control weaknesses are accurately reported, ultimately reducing the risk of security incidents.

VA's continuous monitoring program has achieved significant milestones, including:

- Deployment of a near real-time continuous monitoring capability and process that provides visibility into key security documentation for security updates to include SCAs, risk assessments, and privacy impact assessments, as needed, enabling VA's ability to proactively identify and address potential vulnerabilities.
- Enhanced role-based training for system security personnel, resulting in improved key security control documentation (e.g. system security plans, privacy impact assessments, etc.).
- Standardization of ATO process, ensuring consistency and efficiency in VA's security practices.
- Improved enterprise visibility into system documents and controls, facilitating more informed decision-making and risk management.

- Regular release of action items to the field, promoting timely review and update of key security documentation and ensuring that our security practices remain current and effective.
- Integration of VA System Inventory and governance, risk, and compliance (GRC) tool registration processes, eliminating duplication of legacy data and enabling real-time tracking of system-level security efforts.
- Deployment of an annual self-assessment review capability within the GRC tool, allowing stakeholders to validate control implementation, document test evidence, and implement an accountability structure for system security activity approvals.

Risk-Based Remediation Goals:

In FY 2025, VA will focus on achieving the following risk-based remediation goals:

- Enhance VA's continuous monitoring scorecard automation capabilities to achieve near real-time identification of high-risk vulnerabilities, ensuring significant reduction in exploitable weaknesses and increased compliance with key security documentation by December 31, 2025.
- Establish a process for regularly reviewing and updating key security documentation (SCAs, risk assessments, privacy impact assessments) based on identified risks and changes to the threat landscape by December 31, 2025. Documentation will be updated to reflect current risk posture and inform mitigation strategy as part of the security authorization package.

OIG FISMA Recommendations 4 and 5

Recommendation 4: We recommended the Assistant Secretary for Information and Technology implement improved mechanisms to ensure system owners and Information System Security Officers follow procedures for establishing, tracking, and updating Plans of Action and Milestones (POA&Ms) for all known risks and weaknesses including those identified during security control assessments.

Recommendation 5: We recommended the Assistant Secretary for Information and Technology implement measures to ensure that system stewards and other officials responsible for system level POA&Ms are closing items with relevant support that shows sufficient remediation of the identified weakness.

Comments: Non-concur with recommendations 4 and 5.

Strategic Response and Accomplishments:

VA non-concurs with OIG's recommendations as our analysis indicates that the current POA&M process is effective in managing and mitigating risks associated with identified vulnerabilities. The FY 2024 FISMA audit results demonstrate a high level of compliance, with 99% of POA&M closures containing all necessary documentation to close findings. Furthermore, the low number of site/system findings relative to the population of sampled closed POA&Ms indicates that our risk-based approach to POA&M management is successfully identifying and addressing potential vulnerabilities. Our data-driven approach has enabled us to:

- Identify and prioritize high-risk POA&Ms, ensuring that resources are allocated effectively to address the most critical vulnerabilities.
- Implement changes in the VA GRC tool to prohibit POA&M closure without evidence, thereby enhancing the integrity of our POA&M process.

- Provide continuous training and education opportunities on proper POA&M management and closure, promoting a culture of risk awareness and compliance across the organization.

As a result, we have achieved significant reductions in POA&Ms closed without evidence, with a 90% reduction across the enterprise as of December 2023. The analysis further indicates that the remaining issues with POA&M evidence are limited to localized, system-specific instances already identified in system-level findings, and therefore do not warrant an enterprise-level recommendation.

VA's information technology governance boards track and monitor POA&M key performance indicators (KPI) through monthly reporting and are used as an escalation trigger point into the enterprise risk registry, ensuring that senior executives have visibility into potential risks and can make informed, risk-based decisions. The following KPIs demonstrate the effectiveness of VA's POA&M management process:

- POA&M compliance metric is 90% or higher since October 2024, indicating a high level of compliance and risk management.
- Achieved 90% reduction in ongoing POA&Ms with an age greater than 3 years, demonstrating VA's ability to prioritize and address high-risk vulnerabilities in a timely manner.
- POA&M dashboards provide near real-time monitoring and reporting, enabling us to track progress and identify areas for improvement.

Risk-Based Remediation Goals:

While we non-concur with OIG's initial findings, we are always striving to improve all cybersecurity processes, and as such the following are the future improvement goals for FY 2025:

- Maintaining 90% compliance against identified vulnerabilities without an associated POA&M, ensuring all identified vulnerabilities are properly addressed and mitigated.
- Enforcing risk accepted POA&M process for vulnerabilities that require more than 1 year to complete remediation, as some risks may be inherent and unavoidable, but can still be managed and mitigated through careful planning and monitoring.
- Enhancing GRC capabilities to ensure risk accepted POA&Ms are reviewed annually for critical systems, ensuring that our risk management processes remain current and effective.
- Publishing standardized guidance for substantive POA&M closure evidence, promoting consistency and compliance across the organization.

OIG FISMA Recommendations 6 and 7

Recommendation 6: We recommended the VA Office of Personnel Security, Human Resources, and Contract Offices strengthen processes to ensure appropriate levels of background investigations are performed timely and completed for applicable VA employees and contractors.

Recommendation 7: We recommended the Office of Personnel Security, Human Resources, and Contract Offices implement improved processes for establishing and maintaining accurate investigation data within VA systems used for background investigations.

Comments: Concur with recommendations 6 and 7.

Strategic Response and Accomplishments:

VA concurs with OIG's recommendations. However, VA's implementation of Centralized Adjudication Background Investigation System (VA-CABS) has significantly enhanced our ability to manage and mitigate risks associated with background investigations and adjudications. VA-CABS 2.0 has been integrated with HR-Smart and Account Provisioning and De-provisioning System (APDS) to improve the accuracy and consistency of position designation data, ensuring that employees and contractors are subject to the appropriate level of background investigation. The improvements made to VA-CABS 2.0 have resulted in:

- Automated position designation data, reducing the risk of manual errors and inconsistencies.
- Enhanced reporting capabilities, enabling us to better track and manage background investigation data.
- Improved visibility into contractor background investigation compliance, facilitating more effective risk management.

Achievements include:

- Integration of Automated Classification System with HR-Smart, automating the transfer of position sensitivity and risk designation data elements and ensuring data accuracy and consistency across VA systems.
- Mandatory use of APDS, correlating investigation data across multiple sources to ensure accounts are only provisioned for authorized users.
- Development of interim reports, improving visibility for special user-groups such as contractors and health professional trainees (HPT).
- Initial reviews of investigation levels for all user types in HR-Smart, marking a significant milestone in our risk management efforts.

Risk-Based Remediation Goals:

By September 2026, VA will prioritize the following risk-based remediation goals:

- Validate position designation data for contractors, HPTs, and other user groups, ensuring that 95% of data is accurate and current by December 2025.
- Conduct a comprehensive review of background investigation data to identify potential risks and discrepancies, with a goal of achieving 95% match or exceedance of position designation in VA-CABS for all user types by September 2026.
- Implement additional controls and processes to mitigate the risk of inaccurate or incomplete background investigation data, ensuring that our security practices remain robust and effective by September 2026.

OIG FISMA Recommendations 8 and 9

Recommendation 8: We recommended the Assistant Secretary for Information and Technology ensure contingency plans for all systems and applications are updated and tested in accordance with VA requirements.

Recommendation 9: We recommended the Assistant Secretary for Information and Technology implement improved procedures to ensure that system outages are resolved within stated recovery time objectives.

Comments: Concur with recommendations 8 and 9.

Strategic Response and Accomplishments:

VA concurs with OIG's recommendations as there are areas of improvement specifically with executing test objectives. Although there are findings, VA continues to enhance its contingency planning (CP) efforts by standardizing templates, conducting user trainings, and monitoring the performance of testing to ultimately reduce the risk of operational impacts.

Achievements include:

- Updates to Handbook 6500.8, Information System Contingency Planning, contingency planning controls, standard operating procedures (SOP), and control correlation identifiers to align with National Institute of Standards and Technology (NIST) and federal guidance, ensuring CP practices remain current and effective.
- Issuance of action items requiring all VA systems to review, update, and test information system contingency plans (ISCP) and disaster recovery plans (DRP), promoting a culture of preparedness and risk awareness across the organization.
- Development of a training program for key stakeholders focused on CP testing and operations (e.g. recovery time objectives, etc.), enhancing their knowledge and skills in responding to disruptions and ensuring continuity of critical services.

Risk-Based Remediation Goals:

By March 2026, VA will prioritize the following risk-based remediation goals:

- Maintain compliance with established thresholds for completion and testing of business impact analysis, ISCP, and DRP, prioritizing systems based on system risk profiles and criticality to VA operations. Specifically:
    - 95% compliance for HVA systems, which are critical to patient care and require enhanced protection.
    - 90% compliance for high availability systems, which support essential services and require rapid recovery in the event of a disruption.

OIG FISMA Recommendations 10 and 11

Recommendation 10: We recommended the Assistant Secretary for Information and Technology ensure system owners consistently implement processes for periodic reviews of user account access. Remove unnecessary and inactive accounts on systems and networks.

Recommendation 11: We recommend the Assistant Secretary for Information and Technology coordinate with system owners and local system management to ensure the consistent monitoring and reviewing of privileged accounts, service accounts, and accounts for individuals with access to source code repositories are performed across VA systems and platforms.

Comments: Non-concur with recommendations 10 and 11.

Strategic Response and Accomplishments:

VA non-concurs with OIG’s recommendations, as the results of OIG's review indicate a significant level of maturity in our access management practices, with many systems demonstrating no findings related to

user access review, disablement of inactive user accounts, user access approvals, least privilege, separation checklists, and elevated privilege account monitoring.

Achievements include:

- 72% of systems reviewed had no findings related to user access review, indicating a low risk of unauthorized access. Of those systems that did have findings, 40% of account review issues were identified in one system, allowing us to focus our remediation efforts on a specific area.
- 86% of systems reviewed had no findings related to disablement of inactive user accounts, demonstrating our effectiveness in removing access for inactive users and reducing the risk of unauthorized access. Of the 2,541 accounts identified with disablement issues, 89% were found within one system, allowing us to target our remediation efforts on a specific area.
- 94% of systems reviewed had no findings related to user access approvals or evidence of approvals, indicating a high level of compliance with our access management policies. This reduces the risk of unauthorized access and ensures that all access is properly authorized and documented.
- 96% of systems reviewed had no findings related to least privilege (excess permissions), demonstrating our effectiveness in implementing least privilege principles and reducing the risk of lateral movement. Of the 64 identified accounts with excess permissions, 98% were found within one system, allowing us to focus remediation efforts on a specific area.
- 97% of separations were documented with a checklist, indicating a high level of compliance with our separation procedures, and reducing the risk of unauthorized access. Of the 88 separations identified with no checklist, 50% were found at 4 sites, allowing us to target remediation efforts on specific areas.
- 82% of systems reviewed had no findings related to approvals for privileged access, demonstrating our effectiveness in managing privileged access and reducing the risk of unauthorized access. Of the 53 identified accounts with approval issues, 74% existed within 3 systems, allowing us to focus remediation efforts on specific areas.
- 80% of systems reviewed had no findings related to inactive accounts with privileged access, indicating a low risk of unauthorized access. Of the 2,159 identified inactive accounts with privileged access, 99% were found within one system, allowing us to target our remediation efforts on a specific area.

To further enhance access management practices, VA has achieved the following:

- Enrolled 100% of contractors, HPTs without compensation, and volunteers in APDS, ensuring proper identity management and reducing the risk of unauthorized access.
- Updated VA's Identity, Credential and Access Management (ICAM) Directive and Handbook 6510 to align with regulatory requirements and reflect our enhanced ICAM processes, procedures, and technologies.
- Deployed the account diagnostics tool, which allows information system security officers to view and address deficiencies in account disablement procedures. This has resulted in a 97.5% completion rate for disablement of terminated staff accounts and complete disablement of accounts that have been inactive for over 90 days.

- Continued progress with the implementation of APDS, which serves as a single repository to effectively govern all VA user identities, create digital identities, and manage identity lifecycle events.

Risk-Based Remediation Goals:

We are focused on continuing to mature our access management practices, with the following objectives:

- By December 31, 2025, we will manage 100% of employees in APDS, ensuring that all employee identities are properly managed and reducing the risk of unauthorized access.
- By December 31, 2025, we will manage 100% of accredited representatives/affiliates in APDS, ensuring that all representative identities are properly managed and reducing the risk of unauthorized access.
- By December 31, 2025, we will establish a Workforce Identity Governance and Administration Solution(s) that will serve as a central point to manage separation of duties, establish periodic access reviews of both privileged and non-privileged accounts, validate that user access request forms are completed and authorized in accordance with policy, and enhance workforce user identity lifecycle management.
- By December 31, 2026, we will enroll 100% of enterprise users into the Workforce Identity and Governance Administration Solution(s), ensuring that all user identities are properly managed and reducing the risk of unauthorized access.

By achieving these goals, VA will further mature access management practices, reducing the risk of unauthorized access and improving our overall cybersecurity posture. The risk-based assessment approach has provided actionable guidance on where to focus VA's cybersecurity efforts, enabling us to prioritize and address the most critical security risks.

OIG FISMA Recommendation 12

Recommendation 12: We recommend the Assistant Secretary for Information and Technology implement improved processes to ensure compliance with VA password policy and security configuration baselines on domain controllers, operating systems, databases, application, and network devices.

Strategic Response and Accomplishments:

Comments: Non-concur with recommendation 12. Concur with recommendation 15.

VA's efforts to establish and maintain secure configuration settings continue to mature our process to ensure we have effectively reduced the risk of security breaches and improved overall cybersecurity posture. By providing stakeholders with authorized VA enterprise secure configuration checklists/platform baselines and guidance, we have ensured that all systems are configured to meet established security standards.

Achievements include:

- Ensuring that all published VA enterprise secure configuration checklists/platform baselines have assessment strategies that are properly documented and configured to use enterprise automated monitoring tools where possible, enabling us to identify and remediate potential security vulnerabilities in a timely manner.

- Reconciling all published VA enterprise secure configuration checklists/platform baselines with VA password policy found in the VA Knowledge Service, and obtaining approval from the Office of Information Security for any deviations, demonstrating our commitment to enforcing robust password policies and protecting sensitive information to fully address Recommendation 12.
- Updating and aligning enterprise processes, SOPs, handbooks, and other guidance governing enterprise security baselines, thereby ensuring that our security practices remain current and effective.
- Defining enterprise compliance thresholds and providing guidance on security control deviations within the VA Authorization Requirements SOP, enabling us to measure and track compliance with established security standards.

Risk-Based Remediation Goals:

By March 2027, VA will prioritize the following risk-based remediation goals:

- Collaborate with platform owners to establish processes for maintaining secure configuration settings based on checklists, ensuring that all systems are configured to meet established security standards and reducing the risk of security breaches.
- Develop recommendations for a formal platform configuration manager role to support information system owners/product owners with system-level CM-6: configuration settings control implementation, enabling us to ensure consistent and effective configuration management across all systems.
- Identify and prioritize training needs based on audit findings and support requests, while offering role-based training for those designated as configuration managers, ensuring that our personnel have the necessary skills and knowledge to maintain secure configuration settings.
- Unify system-level compliance reporting for all secure configuration settings, software baselines, and POA&Ms within a single report, providing a comprehensive view of our cybersecurity posture and enabling us to identify areas for improvement.

OIG FISMA Recommendations 13 and 14

Recommendation 13: We recommended the Assistant Secretary for Information and Technology ensure established change control procedures are consistently followed for testing and approval of system changes for VA applications and networks.

Recommendation 14: We recommended the Assistant Secretary for Information and Technology implement and consistently enforce established procedures for preventing and detecting potential unauthorized changes across all platforms and applications in the environment.

Comments: Concur with recommendations 13 and 14.

Strategic Response and Accomplishments:

VA concurs with OIG's recommendations as VA continues to mature the change control processes to demonstrate effectiveness in managing and mitigating risks associated with changes to VA's information technology systems. The mature enterprise change control policy, documented in an enterprise SOP, provides clear guidance for implementation, and ensures that all changes are properly assessed, approved, and implemented.

OIG's findings, which noted issues in 4% of production change request tickets and 11% of pre-production change requests, as well as deficiencies in system-specific pre-production change management process implementation in 8% of systems tested, do not indicate a widespread failure of controls surrounding change control processes. Instead, these findings highlight areas for targeted improvement and refinement of existing processes.

Achievements include:

- Standardization of change control forms to provide testing consistency, ensuring that all changes are evaluated and approved using a consistent framework.
- Completion of onboarding all VA financial systems to the change control program, expanding the scope of our change management processes, and enhancing overall security posture.
- Documentation of issues in POA&Ms and system security plans for systems that do not adhere to enterprise change control policies and procedures, ensuring that these issues are properly tracked and remediated.
- Ongoing training on VA Directive 6004, Configuration, Change and Release Management Programs, which establishes and maintains configuration, change, and release management programs in accordance with NIST Special Publication 800-128, Guide for Security-Focused Configuration Management of Information Systems, promoting a culture of risk awareness and compliance among our personnel.
- Implementation of a change control probation process and distribution of instructions on managing unauthorized emergency change requests, demonstrating our commitment to enforcing change control policies and procedures.
- Implementation of the major incident management process, which improves oversight and accountability for unauthorized changes and enables us to respond quickly and effectively to security incidents.
- Verification that onboarding levels of identified OIT services/systems have remained at or above 95%, ensuring that our change management processes are consistently applied across all systems.
- Maintenance of a low rate (less than 5%) of major incidents caused by changes, with no incidents caused by unauthorized changes noted in OIG's testing, demonstrating the effectiveness of our change control processes in preventing security incidents.

Risk-Based Remediation Goals:

By October 2025, VA will prioritize the following risk-based remediation goals:

- Establish a formal software configuration manager role to support system-level Configuration Management (CM)-2: baseline configuration control implementation and all software development lifecycle phases for each system, ensuring that configuration management is integrated into all aspects of system development and maintenance.
- Define and document roles and responsibilities for identified system stakeholder roles involved with implementation of configuration management controls, promoting clear understanding and accountability among our personnel.

- Establish a software configuration management community of practice to crowd-source development of material and publish it via an integrated portal or hub, facilitating knowledge sharing and collaboration among our personnel.
- Identify and prioritize training needs with a focus on role-based training for software configuration managers, ensuring that our personnel have the necessary skills and knowledge to effectively manage configuration changes and mitigate associated risks.

OIG FISMA Recommendations 12 and 15

Recommendation 15: We recommended the Assistant Secretary for Information and Technology ensure that all systems and platforms are monitored for compliance with documented VA standards for baseline configurations. Ensure that system owners consistently implement and monitor their configurations.

Strategic Response and Accomplishments:

Comments: Non-concur with recommendation 12. Concur with recommendation 15.

VA's efforts to establish and maintain secure configuration settings continue to mature our process to ensure we have effectively reduced the risk of security breaches and improved overall cybersecurity posture. By providing stakeholders with authorized VA enterprise secure configuration checklists/platform baselines and guidance, we have ensured that all systems are configured to meet established security standards.

Achievements include:

- Ensuring that all published VA enterprise secure configuration checklists/platform baselines have assessment strategies that are properly documented and configured to use enterprise automated monitoring tools where possible, enabling us to identify and remediate potential security vulnerabilities in a timely manner.
- Reconciling all published VA enterprise secure configuration checklists/platform baselines with VA password policy found in the VA Knowledge Service, and obtaining approval from the Office of Information Security for any deviations, demonstrating our commitment to enforcing robust password policies and protecting sensitive information to fully address Recommendation 12.
- Updating and aligning enterprise processes, SOPs, handbooks, and other guidance governing enterprise security baselines, thereby ensuring that our security practices remain current and effective.
- Defining enterprise compliance thresholds and providing guidance on security control deviations within the VA Authorization Requirements SOP, enabling us to measure and track compliance with established security standards.

Risk-Based Remediation Goals:

By March 2027, VA will prioritize the following risk-based remediation goals:

- Collaborate with platform owners to establish processes for maintaining secure configuration settings based on checklists, ensuring that all systems are configured to meet established security standards and reducing the risk of security breaches.
- Develop recommendations for a formal platform configuration manager role to support information system owners/product owners with system-level CM-6: configuration settings control

implementation, enabling us to ensure consistent and effective configuration management across all systems.

- Identify and prioritize training needs based on audit findings and support requests, while offering role-based training for those designated as configuration managers, ensuring that our personnel have the necessary skills and knowledge to maintain secure configuration settings.
- Unify system-level compliance reporting for all secure configuration settings, software baselines, and POA&Ms within a single report, providing a comprehensive view of our cybersecurity posture and enabling us to identify areas for improvement.

OIG FISMA Recommendation 16

Recommendation 16: We recommended the Assistant Secretary for Information and Technology implement automated software management processes on all agency platforms to identify and prevent the use of unauthorized software on agency devices.

Comments: Non-concur with recommendation 16.

Strategic Response and Accomplishments:

VA non-concurs with OIG's recommendation, as our robust application monitoring process and application control initiative have effectively mitigated risks associated with unauthorized software usage. OIG's analysis of FY 2024 findings revealed a low failure rate of 0.35% (353 instances out of 98,622 devices reviewed) for deviations not properly documented for the use of non-approved software within the VA Technical Reference Model. The finding demonstrates that our existing controls are effective in preventing enterprise-wide control failures.

OIG did not identify malicious prohibited software on any endpoint within system boundaries, and issues with outdated software were limited to non-maliciously installed programs or applications without proper application controls. These results indicate that our risk-based approach to application monitoring and control is successful in minimizing potential security risks.

Our achievements include:

- Implementation of a robust application monitoring process for Windows systems, covering approximately 90% of all OIT assets, which enables us to detect and respond to potential security incidents in real-time.
- Limitation of software installation to enterprise-approved applications by authorized users, reducing the risk of unauthorized or malicious software being introduced into our environment.
- Implementation of VA's application control initiative through a deny list (blacklist) approach for prohibited software instances on endpoints, which effectively blocks 100% of prohibited applications on Windows-based endpoints and ensures that only approved software is used within our environment.
- Verification that each VA enterprise platform baseline ensures changes, including software installation attempts, are logged and reported to the central security information and event management tool and reviewed by system stakeholders, providing an additional layer of visibility and control over potential security incidents.

- Development of a comprehensive list of approved and unapproved software, which enables us to make informed decisions about software usage and ensures that only authorized software is used within our environment.

Risk-Based Remediation Goals:

By September 2027, VA will prioritize the following risk-based remediation goals:

- Select an application control tool for servers based on a request for information by April 30, 2025, to further enhance our ability to monitor and control software usage on servers.
- Implement and deploy selected application control solutions for Windows workstations deny listing by May 15, 2026, to ensure that workstations only use approved software and to minimize the risk of introducing unauthorized or malicious software into our environment.
- Implement and deploy selected application control solutions for server deny listing by September 30, 2026, to extend our application control capabilities to servers and further reduce potential security risks.
- Implement and deploy selected application control solutions for servers allow listing by September 30, 2027, to enable more granular control over software usage on servers and ensure that only authorized software is used within our environment.
- Implement and deploy selected application control solutions for Windows workstations allow listing by September 30, 2027, to provide an additional layer of visibility and control over software usage on workstations and minimize potential security risks.

OIG FISMA Recommendation 17

Recommendation 17: We recommended the Assistant Secretary for Information and Technology implement improved procedures for establishing, documenting, and monitoring an accurate software and logical hardware inventory for system boundaries across the enterprise.

Comments: Non-concur with recommendation 17.

Strategic Response and Accomplishments:

VA non-concurs with OIG's recommendation regarding logical hardware inventory, as existing processes have demonstrated effectiveness in managing and mitigating risks associated with hardware inventory management. The asset alignment SOP provides a comprehensive framework for identifying connected hardware used to support VA applications and operations, and our implementation of this process has resulted in significant improvements in compliance and accuracy.

While certain FY 2024 audit target sites and systems did not meet the 95% compliance threshold at the time of their onsite audit, we acknowledge that these deficiencies were not due to a lack of process, but rather incomplete implementation of the mature process. We have taken corrective actions to address these issues, including correcting boundary misalignments and tracking remediation efforts in POA&M items.

Achievements include:

- Achieving 98% compliance with enterprise hardware physical inventory requirements, demonstrating our ability to accurately track and manage physical assets.

- Aligning 95% of hardware logical inventory with the correct system authorization boundaries through the FISMA Containerization Asset to Boundary effort, ensuring that our logical inventory is properly aligned with system authorization boundaries.
- Establishing a required enterprise compliance threshold of 95% for monthly asset to boundary alignment validation and achieving this mark within 11 months, demonstrating our commitment to ongoing monitoring and improvement.
- Developing training in support of the monthly validation requirements for connected logical assets, ensuring that our personnel have the necessary skills and knowledge to maintain accurate inventory.
- Improving the accuracy of connected hardware inventory and rolling out automated categorization of asset inventory to all sites across VA, enhancing our ability to track and manage assets.

VA non-concurs with OIG's recommendation regarding software inventory, as our software asset management processes has demonstrated effectiveness in managing and mitigating risks. OIT is in the final stages of transitioning to a comprehensive framework, enterprise Software Asset Management program, that will deploy end-to-end accountability and security measures for software that will further mature software asset management.

Achieved the following:

- Achieved 95% compliance in validation of enterprise software inventory aligned to Office of Management and Budget (OMB) Memorandum M-22-18 (Enhancing the Security of the Software Supply Chain through Secure Software
- Development Practices) requirements, demonstrating our ability to accurately track and manage software assets.
- Improved the accuracy of software inventory and rolled out automated categorization of asset inventory to all sites across VA, enhancing our ability to track and manage software assets.
- Developed enterprise software inventory requirements with 6-month update intervals, ensuring that our software inventory remains current and accurate.
- Established an ongoing reporting process for firmware utilizing available tools, providing visibility into firmware usage, and enabling us to identify potential risks.

Risk-Based Remediation Goals:

By October 2026, VA will prioritize the following risk-based remediation goals:

- Complete intake of designated government off-the-shelf (GOTS) software products into the software asset inventory by October 2025, ensuring that all GOTS software is properly tracked and managed.
- Complete intake of designated cloud provided software products into the software asset inventory by April 2026, ensuring that all cloud-provided software is properly tracked and managed.
- Develop all required policy and compliance documentation to support the foundational software asset management enterprise process by October 2026, providing a comprehensive framework for software asset management.
- Complete intake of designated firmware software products into the software asset inventory by October 2026, ensuring that all firmware is properly tracked and managed.

- Complete intake of designated middleware software products into the software asset inventory by October 2026, ensuring that all middleware is properly tracked and managed.

OIG FISMA Recommendations 18 and 19

Recommendation 18: We recommended the Assistant Secretary for Information and Technology implement improved processes for monitoring and analyzing significant system audit events for unauthorized or unusual activities across all systems and platforms in accordance with VA policy. Ensure privileged activity is monitored on all systems and applications.

Recommendation 19: 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.

Comments: Concur with recommendations 18 and 19.

Strategic Response and Accomplishments:

VA concurs with OIG's recommendation as VA continues to drive maturity in our ongoing efforts to enhance incident response and logging capabilities that will significantly improve our ability to detect, respond to, and mitigate cybersecurity threats.

By completing the alignment of incident response policies and procedures to OMB Memorandum M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents, we have ensured that our incident response processes are consistent with industry best practices and regulatory requirements.

The deployment of an endpoint detection and response capability will enable us to collect valuable telemetry data, which will be used to triage and investigate incidents in a timely and effective manner. This capability will also provide us with enhanced visibility into system events and anomalies, allowing us to respond quickly to potential security threats.

Our progress includes:

- Achieving 79.02% logging coverage for devices that compose systems classified as critical or bedrock, with ongoing efforts to align logging details with OMB Memorandum M-21-31 guidance. This represents a significant increase of 17.29% from the previous mark of 61.73%, demonstrating our commitment to improving the quality and quantity of our logging capabilities.
- Implementing Behavior Analytics with installation planned for approximately 30,000 assets, which will enable us to monitor anomalous activity of users and entities and identify potential security threats in real-time.

Risk-Based Remediation Goals:

By September 2025, VA will prioritize the following risk-based remediation goals:

- Complete 100% alignment of incident response and audit logging policies and procedures to OMB Memorandum M-21-31 by September 30, 2025, ensuring that our incident response processes are fully compliant with regulatory requirements and industry best practices.
- Achieve 100% visibility into VA's cybersecurity logging coverage of bedrock, critical, and internet-facing system assets at Event Logging Level 1 by September 30, 2025, providing us with comprehensive visibility into system events and anomalies, and enabling us to respond quickly to potential security threats.

OIG FISMA Recommendations 20, 22, and 23

Recommendation 20: We recommended the Assistant Secretary for Information and Technology implement improved mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and Web application servers in accordance with established policy timeframes. If patches cannot be applied or are unavailable, other protections or mitigations should be documented and implemented to address the specific risks.

Recommendation 22: We recommended the Assistant Secretary for Information and Technology implement improved processes to require system owners and management to provide adequate credentials to ensure security scans are authenticated to end devices where feasible and the subsequent vulnerabilities are remediated in a timely manner.

Recommendation 23: We recommended the Assistant Secretary for Information and Technology improve the process for tracking and resolving vulnerabilities that cannot be addressed by enterprise processes within policy timeframes. Implement mitigations for identified security deficiencies by applying security patches, system software updates, or configuration changes to reduce applicable security risks.

Comments: Non-concur with recommendations 20, 22, and 23.

Strategic Response and Accomplishments:

VA non-concurs with OIG's recommendations, however, we are committed to maintaining a robust vulnerability management program that aligns with federal and industry standards. The program has consistently demonstrated a high level of effectiveness in managing critical and high vulnerabilities, with a sustained performance of 90% or greater.

To achieve this level of performance, we have implemented several key strategies:

- Established a comprehensive database and web-based vulnerability tracking tool, known as the POA&M Vulnerability Portal. The portal enables the alignment of vulnerabilities with POA&Ms, ensuring visibility, accountability, and proper system owner reviews.
- Use of a risk-based approach to prioritize detected vulnerabilities for remediation and mitigation. This approach considers an asset's business impact, likelihood of vulnerability exploitation, and degree of exposure to adversaries. Additionally, this approach considers known exploited vulnerabilities when determining the likelihood of vulnerability exploitation.

VA's vulnerability management program has achieved several notable successes:

- Remediated 100% of systems across the environment that have Priority 1 vulnerabilities within 14 days.
- Maintained an average of 90% compliance rating in mitigating all critical vulnerabilities across the environment.
- Aligned 90% of assets to system boundaries within the GRC tool, ensuring that assets are evaluated during the assessment and authorization (A&A) process.
- Enforced the A&A process to use credentialed vulnerability assessments in obtaining an ATO.
- Implemented end-of-life (EOL) procedures to ensure that existing EOL platforms and applications are remediated via decommission plans and POA&Ms.
- Implemented a self-service vulnerability scanning solution.

To further enhance the vulnerability management program, VA has established the following remediation goals:

- By September 30, 2025, enforce credentialed scans against 75% or more of assets that support authentication by the enterprise scanning solution within the A&A process.
- By September 30, 2025, update the Enterprise Vulnerability Management Plan to include prioritization language and flaw remediation management for the communication and orchestration of vulnerability management practices at the enterprise level.
- By September 30, 2025, reduce remediation time from 14 days to 7 days for 100% of Priority 1 vulnerabilities that have not been risk accepted by the Department's Chief Information Officer or Chief Information Security Officer.

By achieving these goals, VA will have further enhanced the vulnerability management program, reduced the risk of security breaches, and improved our overall cybersecurity posture. The risk-based assessment approach has provided actionable guidance on where to focus VA's cybersecurity efforts, enabling us to prioritize and address the most critical security risks.

OIG FISMA Recommendation 21

Recommendation 21: We recommended the Assistant Secretary for Information and Technology continue to implement improved segmentation controls that restrict vulnerable medical devices from unnecessary access from the general network.

Comments: Non-concur with recommendation 21.

Strategic Response and Accomplishments:

VA non-concurs with OIG's recommendation, as VA affirms its commitment to robust medical device security through the medical device protection program. OIT has implemented a comprehensive approach to segmenting and protecting networked medical devices, including:

- Risk-based assessment: enterprise risk assessments are conducted on all networked medical devices to identify constraints and tailor compensating security controls.
- Dedicated medical device isolation architecture (MDIA): MDIA segments devices from the general network using virtual local area networks and access control lists, enforced through network access control tools.
- Continuous visibility and monitoring: a comprehensive inventory provides visibility into devices, enabling vulnerability detection, and policy scans continuously improve access control list efficacy.

To further enhance this posture, VA will:

- Advance to Zero Trust isolation architecture: by April 30, 2025, VA will publish a plan for an enhanced isolation architecture aligned with Zero Trust principles.
- Automate inventory and vulnerability management: by June 27, 2025, publish a plan to increase automation of medical device and Internet of Things inventory and vulnerability management, reducing manual effort and improving responsiveness.

These efforts will significantly improve the security and resilience of medical devices, reduce the risk of breaches, and strengthen VA's overall cybersecurity posture. The risk-based approach ensures focused cybersecurity efforts and prioritization of critical risks.

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

OIG reports are available at www.vaoig.gov.