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 2025


| Audit | 25-01698-70 | July 27, 2026 |
|---|---|---|


## OUR MISSION

To conduct independent oversight of the Department of Veterans Affairs that combats fraud, waste, and abuse and improves the effectiveness and efficiency of programs and operations that provide for the health and welfare of veterans, their families, caregivers, and survivors.

## 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:** The Honorable Paul R. Lawrence, PhD, Deputy Secretary of Veterans Affairs, performing the delegable duties of the Assistant Secretary for Information and Technology and Chief Information Officer (005)

**FROM:** Larry Reinkemeyer, Assistant Inspector General
Office of Audits and Evaluations, VA Office of Inspector General (52)

**THRU:** Honorable Cheryl L. Mason, Inspector General
VA Office of Inspector General (50)

**SUBJECT:** Federal Information Security Modernization Act (FISMA) Audit for Fiscal Year (FY) 2025

1. Enclosed is the final report, *Federal Information Security Modernization Act Audit for Fiscal Year 2025*. 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 to 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 2025. CLA will follow up on open recommendations and evaluate the adequacy of corrective actions during its FY 2026 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
    - 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 operate 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 19 recommendations for improving VA's information security program. The FY 2024 FISMA report provided 23 recommendations for improvement. Some recommendations were modified or not closed because relevant information security control deficiencies identified during the FY 2025 FISMA audit were repeat deficiencies. Six prior-year recommendations were closed because VA improved how it monitors controls for contractor systems and how it detects unauthorized vulnerability scans. Two new recommendations were added.
5. VA Office of Information and Technology non-concurred with the recommendations in this FY 2025 report, and the Deputy Secretary of VA, performing the delegable duties of the acting assistant secretary for information and technology and chief information officer, stated that VA believes many of the recommended actions are already underway, already implemented, or do not fully reflect the current state of VA's program. Appendix D provides the full text of VA's response. The effect of the open recommendations will be considered in the FY 2026 audit of VA's information security program.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

# Abbreviations

| | |
|---|---|
| ATO | authority to operate |
| CLA | CliftonLarsonAllen LLP |
| DHS | Department of Homeland Security |
| ECSP | Enterprise Cybersecurity Strategy Program |
| FISMA | Federal Information Security Modernization Act |
| FY | fiscal year |
| GRC | Governance Risk Compliance |
| 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 |
| SDLC | Systems Development Lifecycle |
| SP | Special Publication |

CliftonLarsonAllen LLP
CLAconnect.com

July 17, 2026
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, 2025. 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 24 selected major applications and general support systems hosted at 11 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 2025 through October 2025.

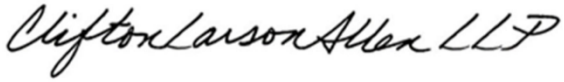
Based on our audit procedures, we concluded that VA continues to face significant challenges meeting the requirements of FISMA. This report provides 19 recommendations to assist VA in strengthening its information security program.

Summarized 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 2025. 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, 2025. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to October 30, 2025. 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
July 17, 2026

# 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 2025 FISMA audit.

# II. Overview

Information security is a high-risk area government-wide. Congress passed the Federal Information Security Modernization Act of 2014 (Pub. L. No. 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 24 major applications and general support systems at 11 VA facilities and the VA Enterprise Cloud. In FY 2025, 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 19 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 2025 FISMA audit were repeat deficiencies. Six (6) prior-year recommendations were closed because VA has made improvements in several control areas. Two (2) new recommendations were added to the report. Appendix A provides more details regarding the closed recommendations. The FY 2024 FISMA report provided 23 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 2025, 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 new 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, and authority to operate processes. 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 Privacy Impact Assessments were not documented or updated in accordance with VA standards.

### Inconsistent Security Control and Privacy Impact Assessments

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. In addition, we identified several instances of Privacy Impact Assessments that were not documented or updated in accordance with VA standards.

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.

## 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 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.)*

### Management Comments

The Deputy Secretary of VA, performing the delegable duties of the acting assistant secretary for information and technology and chief information officer, non-concurred with the

recommendations in the report. In his overall comments, he stated that non-concurrence does not mean VA disagrees that improvements should continue, and stated that VA believes many of the recommended actions are already underway, already implemented, or do not fully reflect the current state of VA's program. He stated that VA made significant progress toward achieving strategic goals in FY 2025, along with key efforts underway which will further strengthen controls and, in many cases, exceed requirements. The Deputy Secretary provided details of those efforts in appendix D.

For recommendation 1, the Deputy Secretary stated that VA's assessment and continuous monitoring processes align with NIST's Risk Management Framework. VA disagrees that NIST requires every security control in the baseline to undergo independent evaluation prior to authorization decisions. The Deputy Secretary stated that VA's approach is consistent with NIST's requirements and emphasis on tailoring, flexibility, and risk informed decision-making throughout the Risk Management Framework. Further, the authorizing official evaluates the results of assessments when making the authority to operate decision. He noted that the Office of Information and Technology (OIT) remains committed to strengthening continuous monitoring capabilities and improving consistency across programs in alignment with NIST requirements.

In response to recommendation 2, the Deputy Secretary reported that VA maintains a robust, risk-based, continuously updated documentation and assessment program that fulfills the intent of the recommendation. He stated that continuous monitoring, independent security control assessments, and automated compliance tools support VA's current processes, and VA's existing documentation and assessment program ensure that security documentation remains accurate, current, and aligned to the operational environment and Federal standards. The Deputy Secretary noted that VA has made substantial progress toward strengthening documentation quality and authorization rigor, and VA considers the residual risk associated with documentation governance to be low. Finally, regarding this recommendation, he said VA performs assessments that are automated, risk-based, and independently validated, and further listed comprehensive goals and milestones for FY 2026 that address the objective of the recommendation.

**OIG Contractor Response**

We agree with the VA's comments regarding recommendation 1 and the tailoring and risk-based prioritization of assessments. The size and complexity of the VA system portfolio coupled with the large surface area of expected controls would increase the need for tailoring and focusing of efforts related to independent control assessments. The condition and recommendation as noted is not intended to target the methodology of the assessments but rather the independence of the assessments as well as the coverage. In the past we noted that ongoing continuous monitoring self-assessments are performed by individuals who are not independent of the systems they support and the group within VA that performs the independent assessments does not have the resources to perform full assessments on all systems undergoing authority to operate (ATO) reviews. While a tailored, risk-based approach in the methodology of independent assessments would allow for more coverage, CLA was not provided with evidence of such focusing of efforts for the independent assessment group.

Regarding recommendation 2, VA's response focuses on performance related to granting ATOs as well as a new Governance Risk Compliance (GRC) application that was not in use in FY 25. The condition and recommendation are focused on the consistent performance and documentation of key security processes and artifacts based on data from the previous GRC. The evaluation of the data in FY 25 indicated that there was inconsistent performance and documentation of certain security processes and artifacts throughout the VA system portfolio. The OIG designated contractor will monitor VA's progress and follow up on implementation of the recommendations until all proposed actions are completed as well as the planned FY 26 milestones identified by the VA.

### 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. Issues were noted related to establishing the appropriate level of background investigations. Without sufficient investigations, especially for individuals with higher risk positions across the enterprise, VA is at risk of allowing individuals to access sensitive data and systems with inappropriate levels of investigation.

## CORRECTIVE ACTIONS RECOMMENDED

3. 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.)*

### Management Comments

The Deputy Secretary non-concurred with recommendation 3, and stated that VA's current processes are mature and automated through the full adoption of Trusted Workforce 2.0 continuous vetting, and that VA's established personnel vetting processes have not demonstrated any systemic deficiencies. He noted that robust controls already in place significantly reduce personnel-related security risk. The Deputy Secretary reported that VA fully transitioned its personnel vetting program to the Trusted Workforce 2.0 model, which replaces legacy periodic reinvestigations with a continuous vetting framework. In addition to the Trusted Workforce Model, he stated that VA employs multiple layers of compensating controls that provide a strong defense-in-depth posture and effectively mitigate risks across the enterprise. Finally, the Deputy Secretary stated that current practices meet or exceed applicable Federal vetting requirements, and VA considers the residual risk associated with personnel vetting and reinvestigation processes to be low. Appendix D provides the full text of the Deputy Secretary's comments.

### OIG Contractor Response

We agree that VA has made significant strides and improvements related to personnel security, background investigations, and continuous vetting. While overall performance significantly improved in our testing results from FY 25, CLA did identify a portion of higher risk positions where investigations were insufficient or not fully completed for personnel. The OIG designated contractor will monitor VA's progress and follow up on implementation of the recommendations until all proposed actions are completed.

### 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 updated and tested in accordance with VA policy requirements.
- We identified several instances of system disruptions and outages related to the VA network and several key applications 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 ensuring consistent recovery from real-world system events to their associated boundaries, VA is at risk of not meeting business recovery objectives when restoring systems in response to a disaster or disruption.

We also noted issues related to the consistent performance and periodic testing of restoration of backup data to ensure integrity and reliability. Without consistently performing and testing system backups, VA is at risk of not being able to fully recover sensitive application information or transactions when system operations are resumed after a disruption.

### CORRECTIVE ACTIONS RECOMMENDED

4. 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.)*
5. 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 repeat recommendation from prior years.)*

6. We recommended the Assistant Secretary for Information and Technology ensure backups are conducted periodically and tested in accordance with established standards for VA system and application data. (*This is a new recommendation.)*

**Management Comments**

The Deputy Secretary non-concurred with recommendations 4, 5, and 6. He stated that the recommendations do not accurately reflect the current maturity level of VA's continuity capabilities or account for the breadth of compensating controls to mitigate risks. He reported that VA employs multiple compensating and preventive controls that meet the intent of the recommendations by directly addressing contingency planning, outage response, and backup integrity, and noted that these enterprise safeguards materially reduce the likelihood of prolonged outages, failed recovery efforts, or inadequate backup execution.

To further enhance governance for contingency planning, the Deputy Secretary reported that VA is integrating contingency planning into a new tool, which exceeds the objective of the recommendations by enabling an improved, proactive governance model. He also noted several milestones for FY 2026. Appendix D provides the full text of the Deputy Secretary's comments.

**OIG Contractor Response**

While CLA acknowledges VA's response and the improvements that have been made to the program, our data from the FY 25 cycle does not support some of the references made in VA's response regarding compensating or mitigating measures. Specifically, for contingency plan updates and testing, the data provided to CLA in FY 25 indicated that 45% of high impact systems did not receive annual functional exercises and that 43% of systems overall had not completed annual testing. Additionally, while VA has comprehensive backup strategies and policies, the audit results from FY 25 indicated that they were inconsistently applied across the sample of systems that were tested. The OIG designated contractor will monitor VA's progress and follow up on implementation of the recommendations until all proposed actions are completed.

**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 and access 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 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 OIT.

### 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.

## CORRECTIVE ACTIONS RECOMMENDED

7. We recommended the Assistant Secretary for Information and Technology ensure system owners consistently implement processes for periodic reviews of user account access and maintain access authorization documentation. Remove unnecessary and inactive accounts on systems and networks. *(This is a repeat recommendation from prior years.)*
8. We recommended the Assistant Secretary for Information and Technology ensure system owners consistently follow termination procedures for the timely disablement of user accounts and the proper completion of termination checklists for separated personnel. *(This is a new recommendation.)*

### Management Comments

The Deputy Secretary non-concurred with recommendations 7 and 8, and stated that VA has implemented extensive enterprise-compensating controls that offer strong prevention, detection, and response capabilities, satisfying the intent of the recommendations. He further noted that enterprise modernization through the Identity Governance Administration solution is in progress, with established timelines and clear governance. The Deputy Secretary stated that VA's existing compensating controls substantially mitigate risks associated with account lifecycle governance, periodic access reviews, and timely removal of access for separated personnel, and the full deployment of VA's modernized Identity Governance Administration capability will further strengthen controls. In the full response, VA noted key controls already in operation, as well as milestones for FY 2026 and 2027 to further enhance access governance. The Deputy Secretary stated that VA remains committed to safeguarding Veteran data and continuously strengthening identity governance. Appendix D provides the full text of the Deputy Secretary's comments.

### OIG Contractor Response

While VA identified several compensating or mitigating measures in its response, the audit results from FY 25 identified deficiencies or risks associated with several of the noted controls. Specifically, the disabling of accounts for unnecessary accounts or separated personnel, the

visibility, coverage, and maturity of audit logging and monitoring tools, and the periodic review or auditing of access privileges were all areas of findings in FY 25. CLA acknowledges the improvements VA has made in these areas. The OIG designated contractor will monitor VA's progress and follow up on implementation of the recommendations until all proposed actions are completed.

**Configuration Management**

Configuration Management testing was performed at the enterprise level and for 24 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 aligned many significant network connected components to the critical system and application boundaries they support. VA had aligned roughly 95% of their network to an associated boundary but many of the remaining unaligned systems were server devices providing significant or critical system functions and services. 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

9. We recommended the Assistant Secretary for Information and Technology work with system owners and change implementers to improve adherence to standards and best practices across the Systems Development Lifecycle (SDLC) for testing and approval of system changes for VA systems and networks. *(This is a modified repeat recommendation from prior years.)*
10. We recommended the Assistant Secretary for Information and Technology work with system owners and application teams to implement and enforce standards for processes related to preventing and detecting potential unauthorized changes across all platforms and applications in the environment. *(This is a modified repeat recommendation from prior years.)*
11. 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.)*
12. 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 repeat recommendation from prior years.)*

13. We recommended the Assistant Secretary for Information and Technology work with system owners to ensure adherence to established procedures for maintaining, 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 Deputy Secretary non-concurred with recommendations 9 and 10, and responded that VA's mature enterprise-wide change management and configuration governance program fulfills the intent of these recommendations. He stated that VA acknowledges opportunities to further strengthen system level consistency. Additionally, he noted that the compensating controls currently in place and active modernization efforts ensure effective change and configuration management oversight across the environment. The Deputy Secretary stated that VA is advancing the maturity of its configuration management program through policy codification, standardized configuration management plans, audit procedures, and automation. He further noted that VA is strengthening system level consistency and audit readiness through planned initiatives to modernize and mature VA's configuration management program beyond the requirements of the recommendations and provided several milestones for FY 2026 through 2029. He reported that VA assesses the residual risk to be moderate due to the scale and distributed nature of VA's systems and ongoing policy codification efforts, and VA remains committed to securing the VA environment.

For recommendation 11, the Deputy Secretary non-concurred and reported that VA's existing controls and planned enhancements demonstrate that its current approach is effective, aligned with risk, and meets Federal expectations. He noted that VA implemented strong defense-in-depth controls. Furthermore, he stated that VA's current practices meet Federal requirements and do not require corrective actions beyond those already in progress to achieve compliance and that VA has plans in place to increase the security of its configuration management posture.

Regarding recommendation 12, the Deputy Secretary non-concurred. He said VA's extensive technical and administrative controls satisfy the intent of the recommendation by preventing unauthorized software. He further noted that VA's planned risk-based modernization efforts are underway, and the combination of safeguards in place provides a level of protection equal to or stronger than a unified automated tool. The Deputy Secretary also noted that VA is strengthening enterprise software governance by establishing measurable strategic milestones that exceed the scope of the recommendation, with planned initiatives for FY 2026 through 2029. He also stated that VA's commitment to continuously enhancing its software asset management posture to safeguard Veteran data and maintain strong compliance with standards.

The Deputy Secretary did not concur with recommendation 13, and stated that current VA processes provide robust inventory, monitoring, and governance—with no demonstrated systemic deficiencies. He noted that VA implemented enterprise-wide processes, governance structures, and compensating controls that address the intent of the recommendation. He also noted that VA remains committed to continuous improvement and will continue enhancing asset management capabilities through continuous authorization monitoring, enterprise software asset

management, and related modernization initiatives. Appendix D provides the full text of the Deputy Secretary's comments.

**OIG Contractor Response**

In regard to recommendations 9 and 10, CLA acknowledges the comprehensive policies, standards, and capabilities that VA has established related to change control and management. While significant strategies and solutions are in place, our FY 25 audit continued to identify inconsistencies in the implementation and enforcement of those policies and standards. Additionally, many of the mitigating or compensating measures listed by VA do not fully address the risk of insufficiently tested changes or unauthorized changes implemented through error, omission, or by internal or external threat actors.

In regard to recommendation 11, several of VA's identified compensating or mitigating measures were either not in place during the FY 25 audit or do not specifically address the risk of inconsistent baseline application and enforcement. For example, the integration of performance indicators into the Service Now Risk Management module was not a control or operation in place during the FY 25 audit. Additionally, deployment standards and hardening guides provide for the secure initial configuration of systems upon deployment but do not necessarily address the risk of configuration drift.

In regard to recommendation 12, VA's response is largely centered around its capabilities present on major platforms and systems as well as several initiatives that were either ongoing and not fully implemented during FY 25 or planned for future cycles. The initial condition and recommendation were oriented around the implementation of allow-listings for high impact systems and the use of automation in specific platforms and specialized purpose and medical systems where many of the tools and capabilities listed in VA's response were not operating in FY 25. There is also not an expectation by the OIG of a single unified tool or capability to supply automation.

In regard to recommendation 13, several of the compensating measures identified by VA were either not in place, were still being implemented or improved, or evidence supporting their implementation was not made available during FY 25. For example, the new governance risk and compliance tool for authorization monitoring was not in place during the FY 25 cycle. Additionally, CLA received evidence indicating that the software asset management program, including the full implementation of the software license accountability solutions, were still undergoing initiatives for implementation and improvement during the FY 25 cycle. While CLA acknowledge that ongoing efforts undertaken by the VA may directly address the recommendations, we cannot evaluate future state capabilities during a current audit cycle. The OIG designated contractor will monitor VA's progress and follow up on implementation of the recommendations until all proposed actions are completed.

**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 all systems VA has categorized as "Critical" or "Bedrock." 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

14. 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. *(This is a modified repeat recommendation from prior years.)*
15. 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 Deputy Secretary non-concurred with recommendations 14 and 15, and said the existing enterprise Security Information and Event Management, logging, correlation, and monitoring capabilities already fulfill the intent of the recommendations. He noted VA's alignment with OMB requirements and said a centralized log review is already operational and continues to expand. He added that strategic initiatives underway will further enhance visibility, detection, and enterprise-wide logging coverage beyond the scope of the recommendations. The Deputy Secretary responded that VA has planned and resourced additional modernization to strengthen audit logging and monitoring, which will further reduce the likelihood of undetected breaches. He noted VA's ongoing commitment to continuously enhance its cybersecurity monitoring posture and effectively capture, analyze, and act upon audit events across all systems and platforms. Appendix D provides the full text of the Deputy Secretary's comments.

### OIG Contractor Response

While CLA acknowledges that VA has made significant enhancements to its logging and monitoring capabilities in recent years, our FY 25 audit continued to identify gaps in visibility for logging, specifically among the population of servers throughout the environment as well as for the OMB logging requirements for Critical and Bedrock systems. VA cited several planned and ongoing improvements to its existing logging and monitoring capabilities. The OIG designated contractor will monitor VA's progress and follow up on implementation of the recommendations until all proposed actions are completed.

### 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 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 by VA.

### 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 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 efforts to isolate medical devices from general network traffic in line with established security 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 from 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, 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

16. 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 repeat recommendation from prior years.)*
17. We recommended the Assistant Secretary for Information and Technology continue to implement controls that restrict vulnerable medical devices from unnecessary access from the general network. *(This is a modified repeat recommendation from prior years.)*
18. 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.)*
19. 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. Additionally, VA should enhance their process for updating baseline images to ensure aged vulnerabilities are not introduced into the environment. *(This is a modified repeat recommendation from prior years.)*

### Management Comments

The Deputy Secretary non-concurred with recommendations 16, 18, and 19, and responded that VA meets or exceeds all authenticated scanning thresholds, which satisfies the intent of the recommendations, and said point-in-time scans are not a good measure of VA's continuous

vulnerability management performance, policy compliance, or remediation timeliness. He stated that VA's mitigating strategies and compensating controls effectively address un-patchable vulnerabilities, and future risk-based initiatives exceed the scope of the recommendations and demonstrate continued program maturity. The Deputy Secretary also noted that in instances when VA cannot immediately patch or otherwise defer vulnerabilities, VA takes appropriate mitigation measures. In the response, he listed compensating controls that strengthen outcomes and noted initiatives for FY 2026 that further strengthen remediation timeliness and authenticated scanning.

The Deputy Secretary also non-concurred with recommendation 17, and stated that VA isolates medical devices from the general network through access control list restricted virtual local area networks and deny-by-default communication policies. He said existing protections fulfill the intent of the recommendation and effectively mitigate risks associated with vulnerable medical or Internet of Medical Things devices. The response listed key controls and noted that VA is also strengthening its isolation architecture through significant strategic initiatives through FY 2029. The Deputy Secretary reiterated VA's commitment to protecting all medical devices and ensuring safe, secure, and uninterrupted clinical operations. Appendix D provides the full text of the Deputy Secretary's comments.

**OIG Contractor Response**

We agree VA has significant mechanisms and programs in place supporting the identification, remediation, and management of vulnerabilities. While our scans are performed at a point in time and cannot identify the length that the vulnerability has been on the network, we still report vulnerabilities that have been known and published for significant periods of time and in some cases which have been known to be exploited previously. The process for identifying and removing vulnerabilities may be outpacing the process for updating device configurations and images for deployment to avoid introducing vulnerable components and software. While VA identifies several mitigations such as plans of actions and milestones, Intrusion Detection Systems, and logging, CLA did not always find that these items directly mitigate the risk of the vulnerabilities reported. The OIG designated contractor will monitor VA's progress and follow up on implementation of the recommendations until all proposed actions are completed.

# Appendix A: Status of Prior-Year Recommendations

We noted 17 of 23 prior-year recommendations are repeated or modified and remain open within the body of this report. As noted in the table below, six recommendations were closed during the FY 2025 FISMA audit.

**Table A.1. Closed Prior-Year Recommendations**

| Number | Recommendation | Status | Corrective actions |
|---|---|---|---|
| FISMA-2024-03 | *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.* | Closed | This recommendation was closed because the associated issues were not noted during the FY 2025 assessment. |
| FISMA-2024-04 | *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.* | Closed | This recommendation was closed because the associated issues were not noted during the FY 2025 assessment. |
| FISMA-2024-05 | *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.* | Closed | This recommendation was closed because the associated issues were not noted during the FY 2025 assessment. |
| FISMA-2024-07 | *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.* | Closed | This recommendation was closed because the associated issues were not noted during the FY 2025 assessment. |

| Number | Recommendation | Status | Corrective actions |
|---|---|---|---|
| FISMA-2024-11 | *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.* | Closed | This recommendation was closed because the associated issues were not noted during the FY 2025 assessment. |
| FISMA-2024-12 | *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.* | Closed | This recommendation was closed because the associated issues were not noted during the FY 2025 assessment. |

# 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 January 2025, OMB issued Memorandum M-25-04, *Fiscal Year 2025 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 2025, the metrics consisted of the core metrics and FY 2025 supplemental metrics.

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 2025. 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 24 selected major applications and general support systems hosted at 11 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.

**Site Selections**

In selecting VA facilities for testing, we considered the geographic region, size, and complexity of each hosting facility, as well as the criticality of systems hosted at the facility. Sites selected for testing included:

- VA Medical Facility – Albuquerque
- VA Medical Facility – Ann Arbor
- VA Regional Office – Atlanta
- VA Medical Facility – Baltimore
- VA Medical Facility – Denver
- VA Medical Facility – Durham
- VA Medical Facility – Fayetteville
- Cyber Security Operations Center and Capital Region Readiness Center – Martinsburg
- VA Regional Office – Seattle
- VA Regional Office – Tampa
- VA Medical Facility – Wichita
- VA Enterprise Cloud – Virtual

We evaluated mission-critical systems that support VA's core mission and business functions. 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: VA Management Comments, Assistant Secretary for Information and Technology

**Department of Veterans Affairs Memorandum**

Date: April 2, 2026

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

Subj: Office of Inspector General Draft Report, Federal Information Security Modernization Act Audit for Fiscal Year 2025 (VIEWS 14387241)

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

1. Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft report, *Federal Information Security Modernization Act Audit for Fiscal Year 2025.*

2. The Office of Information and Technology (OIT) is committed to security excellence, including maintaining a strong information security program to ensure the adequacy and effectiveness of the Department of Veterans Affairs' (VA) information security controls in compliance with the Federal Information Security Modernization Act.

3. OIT is submitting the attached written comments, in which OIT respectfully non-concurs with the report's 19 recommendations related to the Department's information security program. VA maintains controls that already address the intent of the recommendations, along with key efforts underway which will further strengthen controls and, in many cases, exceed requirements.

| *The OIG removed point of contact information prior to publication.* |
|---|

(Original signed by)

Paul R. Lawrence, PhD

Attachment

Attachment

**Office of Information and Technology (OIT)**
**Responses to**
**Office of Inspector General (OIG) Draft Report: Federal Information Security Modernization Act (FISMA) Audit for Fiscal Year (FY) 2025**

*Prior to publication, the OIG revised sensitive information in the interest of operational security. These revisions are indicated by brackets. The OIG maintains the complete text of the attachment.*

Thank you for the opportunity to review the OIG report on the FISMA Audit for FY 2025. Collaboration between VA and OIG during the audit cycle underscores the commitment of VA's OIT to security excellence, while highlighting the importance of VA's continued partnership with OIG's security audit team.

VA non-concurred with the audit's recommendations because many of the findings did not fully account for the security controls, monitoring, and processes already in place across the Department. The audit captured a snapshot in time, while VA manages cybersecurity continuously through ongoing monitoring, automated tools, and risk-based decision making.

Non-concurrence does not mean VA disagrees that improvements should continue. It means VA believes many of the recommended actions are already underway, already implemented, or do not fully reflect the current state of VA's cybersecurity program.

VA remains focused on continuing to strengthen cybersecurity and reducing risk to Veteran services and data.

In FY 2025, VA made significant progress toward achieving strategic goals through a risk-based approach to protecting Veterans' data and ensuring the confidentiality, integrity, and availability of essential services. The control responses and remediation plans outlined in VA's FISMA audit response are a direct result of OIT's continued focus on risk management and VA's mission. OIT will continue to allocate resources to areas that pose the greatest risk to VA's systems and data and that directly impact the Department's 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. Specifically, VA has made notable strides throughout FY 2025 to strengthen cybersecurity in the following areas:

- **Continuous Monitoring and Authorization Improvements:**
    - Achieved a record high of 3-year authorities to operate and increased 2-plus-year authorities to operate from 46.7% to 63.9%. Improvements in this area demonstrate sustained control performance, reduce reauthorization overhead, improve audit readiness, and ensure alignment with ongoing authorization decisions within the National Institute of Standards and Technology's (NIST) Risk Management Framework.
    - Transitioned over [number] system boundaries to the [monitoring] tool. The transition enables near real-time control evidence collection and earlier detection of compliance gaps, while accelerating VA's ability to reduce residual risk by creating and closing plans of action and milestones.

  - Reduced plans of action and milestones aged over 1-year by 93%, which significantly improves remediation timelines, lowers enterprise risk, and increases the Department's FISMA maturity.

- **Supply Chain Risk Management Program:**
  - Completed VA Directive 6519, Cybersecurity Supply Chain Risk Management Strategy, and the accompanying concept of operations. Directive 6519 establishes formal governance and accountability for supply chain risk management, which will enable VA to consistently implement supply chain risk controls and achieve measurable oversight across acquisitions.
  - Developed vendor risk analytics tools for executive level visibility. The tools provide risk scoring and prioritization so leaders can act on high-risk suppliers, while also reducing exposure and informing contract decisions.
  - Assessed supply chain risk posture for 50% of VA's critical vendors. The assessments allow VA to implement targeted remediation plans and contract clauses for the highest risk vendors, which reduces unknown risks by half.
  - Published documented vendor risk assessment procedures and initiated supply chain risk control implementation. Improvements in this area standardize evaluations and accelerate adoption of supply chain risk controls in procurements and system integrations.
- **Identity and Access Management Modernization:**
  - Granted authority to operate for the new Identity Governance Administration solution. The solution will enable automated lifecycle and access reviews, allowing VA to lower orphaned account risk and strengthen compliance.
  - Began to integrate high-critical systems and systems with repeat audit findings with the Identity Governance Administration solution. VA is targeting the highest risk areas first to reduce repeat findings and accelerate remediation.
  - Set goal to enroll 100% of enterprise identities into the Identity Governance Administration solution by [late] 2026. Meeting this goal will ensure uniform governance and measurable enterprise coverage for access controls.
- **Incident Response and Audit Logging:**
  - Aligned incident response policies with the requirements of Office of Management and Budget (OMB) Memorandum M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents. As a result, VA implemented 1-hour security incident reporting, which improves reporting timeliness, escalation, dwell time, and impact.
  - Implemented centralized logging and monitoring in [enterprise tool], which improves detection and response capabilities. Centralized logging and monitoring increases coverage and correlation, enabling faster threat detection and response across platforms.
  - Deployed advanced Security Information and Event Management solutions and automated log analysis tools for anomaly detection. The solution expands detection of suspicious activity, decreases manual burden, and improves incident triage.

**FISMA Recommendations and VA Response:**

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

**VA Comments:** VA non-concurs with recommendation 1. VA's assessment and continuous monitoring processes align with NIST's Risk Management Framework. VA disagrees that NIST requires every security control in the baseline to undergo independent evaluation prior to authorization decisions.

NIST Special Publication 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, specifies that organizations must: a) assess the selected and implemented controls necessary to determine whether they are operating as intended prior to authorization, and b) tailor the control baseline and assessment scope based on system categorization, mission and business requirements, and organizational risk tolerance. Additionally, NIST Special Publication 800-53A, Assessing Security and Privacy Controls in Information Systems and Organizations**,** requires that assessment procedures be customizable and risk-based, which enables agencies to scope assessment activities according to a system's specific risk profile. In short, the NIST requirement is to assess selected and implemented controls for a system consistent with organizationally approved tailoring.

VA's approach is consistent with NIST's requirements and emphasis on tailoring, flexibility, and risk informed decision-making throughout the Risk Management Framework. The authorizing official evaluates the results of assessments when making the authority to operate decision.

Key controls include the following:

- Security control assessments. Assessments ensure the implementation of the required controls for authorization.
- Tailored assessment plans. VA tailors assessment plans in alignment with risk.
- Continuous monitoring activities. Through these activities, VA assesses control effectiveness on an ongoing basis rather than one time prior to authorization.

OIT remains committed to strengthening continuous monitoring capabilities and improving consistency across programs in alignment with NIST requirements.

**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 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.)***

**VA Comments:** VA non-concurs with recommendation 2. VA maintains a robust, risk-based, continuously updated documentation and assessment program that fulfills the intent of the recommendation. Continuous monitoring, independent security control assessments, and automated compliance tools support VA's current processes. VA's existing documentation and assessment program ensure that security documentation remains accurate, current, and aligned to the operational environment and Federal standards.

VA has made substantial progress towards strengthening documentation quality and authorization rigor. In FY 2025, VA achieved a record high number of 3-year authorities to operate while also significantly increasing 2-plus-year authorities to operate from 46.7% to 63.9%. VA's accomplishments in this area demonstrate that VA's controls maintain a sustained and validated performance over time, reflecting the effectiveness of VA's existing continuous monitoring processes.

VA transitioned more than [number] system boundaries into the [monitoring] tool. The transition enables near real-time control evidence, automated artifact collection, and earlier detection of documentation inaccuracies. Improvements in this area directly accelerate OIT's ability to update security control assessments, privacy impact assessments, and other key security artifacts, which materially reduces documentation drift.

Multiple compensating controls mitigate the risk of outdated or inaccurate documentation by ensuring accuracy and effective control evaluation.

Key controls include the following:

- Automated assessment tools. Tools—including security content automation protocol compliant vulnerability scanners, configuration checkers, and compliance-as-code baselines—allow VA to continuously validate configurations and identify deviations requiring documentation updates.
- Risk prioritized penetration testing. Testing—including of high value assets, internet facing systems, and systems lacking recent independent security control assessments—ensures high risk environments receive timely and targeted evaluation.
- Prompt adjudication and plans of action and milestones management. VA's controls in this area prevent prolonged exposure and ensure documentation remains current with remediation efforts.
- Security awareness and phishing resistance training. Training strengthens human factor controls and supports accurate representation of operational risks.

In addition to the controls already in place, VA established comprehensive goals for FY 2026 that address the objective of the recommendation. The goals reflect VA's mature, structured, and measurable documentation governance program.

Milestones for FY 2026 include the following:

- 100% of reportable systems undergoing an authority to operate will have an independent control assessment. Reaching this target will ensure objectivity and alignment with the requirements of the NIST Risk Management Framework.
- 100% of key security documentation for critical systems will be current. This action will ensure that high risk systems artifacts remain accurate and audit ready.
- 100% of all FISMA-reportable systems will have current and accurate documentation. This action will provide enterprise-wide visibility and reduce audit findings.
- FISMA-reportable systems will maintain 100% continuous annual accuracy, year-over-year. This action will institutionalize ongoing compliance and eliminate documentation drift.

VA considers the residual risk associated with documentation governance to be low. VA performs assessments that are automated, risk-based, and independently validated. VA also maintains ongoing documentation currency and has enterprise governance structures aligned with Federal requirements.

**Recommendation 3: 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.)***

**VA Comments:** VA non-concurs with recommendation 3. VA's current processes are mature and automated through the full adoption of Trusted Workforce 2.0 continuous vetting. VA's established personnel vetting processes have not demonstrated any systemic deficiencies. Robust controls already in place significantly reduce personnel-related security risk.

VA fully transitioned its personnel vetting program to the Trusted Workforce 2.0 model, which replaces legacy periodic reinvestigations with a continuous vetting framework. Under Trusted Workforce, real-time automated record checks, monitoring, and adjudication replace traditional reinvestigations. NIST and the Federal Personnel Vetting Council have identified this approach as the appropriate model for modern Federal personnel security. Because the legacy model of periodic reinvestigation no longer applies under Trusted Workforce 2.0, the recommendation does not reflect current Federal personnel vetting policy or VA's operational model.

VA's implementation of Trusted Workforce continuous vetting demonstrated no process failures, systemic noncompliance, or specific deficiencies. Isolated audit observations do not demonstrate that VA's personnel security processes require additional standardization beyond established Federal requirements. A point-in-time audit is not a reliable measure of the effectiveness of VA's ongoing, real-time monitoring system under the Trusted Workforce model.

VA performs rigorous background investigations for all new hires, including identity verification and criminal history checks. VA also maintains a real-time continuous evaluation process for the existing workforce, including continuous record monitoring, automated data checks, incident reporting, training, and periodic reviews.

Concurrently with the Trusted Workforce Model, VA employs multiple layers of compensating controls that provide a strong defense in depth posture and effectively mitigate risks associated with personnel security and suitability across the enterprise.

Key controls include the following:

- Strong identity assurance. Biometric verification and multifactor authentication help ensure only fully vetted individuals can access VA systems, which reduces the risk of impersonation or credential compromise.
- Ongoing activity monitoring. Enterprise audit logging and behavior-based monitoring detect anomalous actions early, reducing the likelihood that insider threat activity or policy violations will go unnoticed.
- Policy enforcement and mandatory training. Clearly defined security requirements, ethics training, and annual security awareness training reinforce personnel accountability, reduce human error, and decrease social engineering risk.
- Principle of least privilege and role-based access control. VA tightly constrains access to data and systems based on job relevance. Access controls minimize potential harm in the event of compromised credentials or insider misuse.

- Contractor agreements and oversight. Strict contract language ensures third party personnel meet Federal vetting requirements and comply with security standards, reducing supply chain and external personnel risk.
- Automated data validation. VA implemented a data application programming interface in FY 2025 to synchronize position information between VA's [systems]. Data validation reduces classification errors and ensures VA provisions personnel with the correct access aligned to their job functions.

Current practices meet or exceed applicable Federal vetting requirements. As a result, VA considers the residual risk associated with personnel vetting and reinvestigation processes to be low.

**Recommendation 4: 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.)***

**Recommendation 5: 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 repeat recommendation from prior years.)***

**Recommendation 6: We recommended the Assistant Secretary for Information and Technology ensure backups are conducted periodically and tested in accordance with established standards for VA system and application data.** ***(This is a new recommendation.)***

**VA Comments:** VA non-concurs with recommendations 4,5, and 6. The recommendations do not accurately reflect the current maturity level of VA's continuity capabilities or account for the breadth of compensating controls to mitigate risks. VA maintains a fully operational and federally compliant continuity and recovery program. VA's program is supported by documented key performance indicators, enterprise backup resiliency, robust monitoring, and continuous authorization monitoring-driven automation.

VA employs multiple compensating and preventive controls that meet the intent of the recommendations by directly addressing contingency planning, outage response, and backup integrity. Enterprise safeguards materially reduce the likelihood of prolonged outages, failed recovery efforts, or inadequate backup execution.

Key controls include the following:

- Annual testing, training, and exercises. VA mandates annual testing, training, and exercises for all information system contingency plans and disaster recovery plans, aligned to Federal Information Processing Standard 199 impact levels. VA's compliance key performance indicators are 95% for high value assets, 90% for high availability systems, and 85% for moderate low systems. VA's requirements ensure validated recovery capability and meet Federal continuity standards.
- Comprehensive enterprise backup strategies. Strategies include incremental and differential backups, 24/7 cross-datacenter replication, and cloud infrastructure services. Enterprise backup strategies ensure data recoverability and sustained availability of mission critical services.
- Strict access controls and monitored restoration operations. These measures reduce insider threats and ensure compliance with Federal data protection standards.

- Enterprise alerting, user activity monitoring, and network segmentation. These measures provide early detection, containment, and rapid response to operational disruptions, resulting in reduced outage duration and improved recovery time objective adherence.
- Information system contingency plan knowledge service. VA continues to expand the information system contingency plan knowledge service, which provides standardized templates, training, and tools to support consistent information system contingency plan and disaster recovery plan development, testing, and execution. Mandated information system contingency plan training for responsible personnel further enhances readiness.

To further enhance governance for contingency planning, VA is integrating contingency planning activities into the [monitoring] tool. The capabilities of this tool exceed the objective of the recommendations by enabling an improved, proactive governance model.

Milestones for FY 2026 include the following:

- The Continuous Authorization Monitoring tool will automate enterprise action items, prompting stakeholders to meet required information system contingency plan and disaster recovery plan development updates and annual testing obligations.
- Within the Continuous Authorization Monitoring tool, automated information system contingency plan and disaster recovery plan templates will improve documentation accuracy and accelerate creation of required artifacts.
- The Continuous Authorization Monitoring tool will monitor testing compliance and provide actionable performance reporting for leadership enforcement.
- The Continuous Authorization Monitoring tool will also track real world recovery performance, enabling VA to validate adherence to system specific recover time objective and recovery point objective requirements.

VA's existing contingency planning posture, backup program, infrastructure redundancy, and Continuous Authorization Monitoring enabled governance enhancements are strong. As a result, VA assesses the residual risk associated with contingency planning, outage response, and backup integrity to be low.

**Recommendation 7: We recommended the Assistant Secretary for Information and Technology ensure system owners consistently implement processes for periodic reviews of user account access and maintain access authorization documentation. Remove unnecessary and inactive accounts on systems and networks.** ***(This is a repeat recommendation from prior years.)***

**Recommendation 8: We recommended the Assistant Secretary for Information and Technology ensure system owners consistently follow termination procedures for the timely disablement of user accounts and the proper completion of termination checklists for separated personnel.** ***(This is a new recommendation.)***

**VA Comments:** VA non-concurs with recommendations 7 and 8. VA has implemented extensive enterprise compensating controls that offer strong prevention, detection, and response capabilities, satisfying the intent of the recommendations. Enterprise modernization through the Identity Governance Administration solution is in progress, with established timelines and clear governance.

VA employs a comprehensive and multilayered identity and access control environment. VA's existing compensating controls substantially mitigate risks associated with account lifecycle governance, periodic access reviews, and timely removal of access for separated personnel. Collectively, the controls in place materially reduce the likelihood of inappropriate access, privilege misuse, or unreviewed accounts. The

full deployment of VA's modernized Identity Governance Administration capability will further strengthen controls.

Additionally, VA enforces a layered set of compensating controls that mitigate risks associated with account disablement and termination checklist compliance. Existing measures minimize the risk associated with isolated checklist delays.

Key controls already in operation include the following:

- Mandatory multi-factor authentication and centralized identity and access management governance. These measures add multiple layers of identity assurance, strengthen access control, and reduce credential compromise risk.
- Automated scripts that deactivate dormant accounts. Automated scripts reduce exploitation risk and shrink the attack surface.
- Comprehensive logging and monitoring. Logging and monitoring enable rapid detection of anomalous behavior and insider threats.
- Independent security audits and role-based access control enforcement. These measures ensure VA consistently maintains least privilege user access across systems.
- Continuous security awareness and phishing resistance training. Training reduces human factor vulnerabilities and supports access documentation for audit readiness.
- Automated account disabling upon termination. This measure prevents unauthorized post-employment access.
- Role-based access controls. Controls strictly limit access to systems required based on job roles.
- Regular access audits. Audits identify and remove accounts for separated employees.
- Multifactor authentication, encryption, and network segmentation. These measures limit exploitation opportunities, even if residual accounts temporarily remain active.
- Endpoint management and remote wipe capabilities. Controls prevent users from obtaining access through devices after separation.
- Incident response procedures. These procedures rapidly mitigate any unauthorized access discovered post-separation.

VA initiated a major modernization effort to further enhance access governance.

Milestones for FY 2026-27 include the following:

- VA granted an authority to operate to the Identity Governance Administration solution in FY 2025 Quarter 2. VA is integrating the solution with high criticality systems and systems with repeat audit findings.
- Integration with the Integrated Financial and Acquisition Management System began in March 2026, targeting one of VA's highest risk and highest visibility environments.
- Integrations with Active Directory and Master Person Index in FY 2026.
- Enrollment of 100% of enterprise identities into the Identity Governance Administration solution by [late] 2026. This action will enable automated access provisioning, deprovisioning, and

periodic reviews. Phased deployment ensures both coverage and accuracy while improving audit defensibility and operational consistency.

VA's wide breadth of compensating controls is highly effective. Controls include multifactor authentication, centralized identity and access management, dormant account automation, role-based access controls, continuous monitoring, encryption, segmentation, endpoint management, and automated termination workflows. These controls materially reduce the likelihood of unauthorized access, privilege escalation, or misuse related to either periodic access reviews or account termination procedures. As a result, VA determined the residual risk for both recommendations to be low, with the risk mitigated by layered defenses and active audit readiness improvements.

VA remains committed to safeguarding Veteran data and continuously strengthening identity governance across the Department.

**Recommendation 9: We recommended the Assistant Secretary for Information and Technology work with system owners and change implementers to improve adherence to standards and best practices across the Systems Development Lifecycle (SDLC) for testing and approval of system changes for VA systems and networks.** ***(This is a modified repeat recommendation from prior years.)***

**Recommendation 10: We recommended the Assistant Secretary for Information and Technology work with system owners and application teams to implement and enforce standards for processes related to preventing and detecting potential unauthorized changes across all platforms and applications in the environment.** ***(This is a modified repeat recommendation from prior years.)***

**VA Comments:** VA non-concurs with recommendations 9 and 10. VA's mature enterprise-wide change management and configuration governance program fulfills the intent of both recommendations. While VA acknowledges opportunities to further strengthen system level consistency, the compensating controls currently in place—enhanced by active modernization efforts—ensure effective change and configuration management oversight across the environment.

VA uses robust enterprise change management controls. OIT documented the production enterprise change management process in an enterprise standard operating procedure. The process provides clear and enforceable guidance to ensure VA appropriately assesses, approves, executes, and tracks all production changes. VA's established enterprise change management controls enforce structured assessment, approval, testing, and enterprise change advisory board governance. Separation of duties, [enterprise tool] workflows, automated testing, rollback procedures, and oversight through change control boards and the enterprise change advisory board mitigate the risk of unauthorized changes.

Simultaneously, VA is advancing the maturity of its configuration management program through policy codification, standardized configuration management plans, audit procedures, and automation. Progress in this area demonstrates VA's strong, ongoing commitment to governance of the systems development lifecycle.

OIT's configuration management framework applies structured governance across the systems development lifecycle. Governance provides information system owners, configuration managers, and change implementation teams with standardized expectations for control performance. VA uses the framework to guide consistent configuration practices across the Department.

VA's enterprise workflows—particularly the integration of [enterprise tool] information technology management change control—ensure centralized governance over production changes, automatic

routing of required approvals, documentation of rationale, review, and authorization, traceability of implementers and approvers, and enforcement of segregation of duties and access control. These capabilities directly mitigate the risk of unauthorized changes across systems and platforms.

VA also takes disciplinary action for non-compliance with change control processes or changes resulting in major information technology incidents, which reinforces adherence to enterprise change requirements.

The controls currently in place substantially prevent unauthorized changes and ensure that system modifications follow established change approval rigor.

Key controls already in operation include the following:

- Segregation of duties and [enterprise tool] approval workflows. Workflows separate authorization, implementation, testing, and approval workflows, which reduces the likelihood of unauthorized or untested changes.
- Automated systems development lifecycle processes supplemented by manual approval gates at critical checkpoints. Automated processes and manual approval gates ensure that VA validates security controls before deployment.
- Clearly defined stakeholder roles and responsibilities for secure configuration management. Roles and responsibilities ensure accountability, governance, and consistent policy adherence.
- Automated testing tools and rollback procedures. These tools and procedures prevent outages, ensure functional integrity, and minimize operational impact in the event of change failure.
- Change control board oversight and enterprise change advisory board governance. Oversight and governance ensure system level and enterprise level visibility, structured approval, and change accountability.

VA is strengthening system level consistency and audit readiness through planned initiatives to modernize and mature VA's configuration management program beyond the requirements of the recommendations. Collectively, these initiatives demonstrate that VA has already established and is executing a structured remediation roadmap.

Milestones for FY 2026-29 include the following:

- Codifying OIT's configuration management framework into enterprise policy.
- Developing and standardizing a system level configuration management plan template for system owners.
- Creating new templates for configuration management and systems development lifecycle standard operating procedures.
- Developing a configuration management assessment procedure, audit template, and remediation action plan framework.
- Implementing configuration management database automation utilities.
- Delivering enterprise-wide configuration management training materials and sessions.

The combination of strong enterprise change governance, mature approval workflows, automated testing, defined roles, and escalating accountability mechanisms ensures that the risk of unauthorized or improperly tested changes remains controlled and monitored. Given the controls in place, VA assesses the residual risk associated with change and configuration management to be moderate. The moderate

risk determination is not a result of deficiencies in protection, but due to the scale and distributed nature of VA's systems and ongoing policy codification efforts. The controls currently in place effectively mitigate risk while the enterprise moves toward full configuration management standardization.

VA remains committed to securing the VA environment, improving systems development lifecycle consistency, and strengthening configuration governance across all systems and applications.

**Recommendation 11: 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.)***

**VA Comments:** VA non-concurs with recommendation 11. VA's existing baseline governance processes, monitoring, compensating controls, and planned enhancements satisfy the intent of the recommendation. The recommendation does not reflect the maturity, structure, breadth, or effectiveness of VA's baseline management and configuration management programs.

VA has established governance, monitoring processes, compensating controls, and enterprise accountability structures designed to ensure baseline compliance. VA implemented a comprehensive baseline management framework to monitor baseline compliance across platforms consistent with Federal requirements. The existing controls and planned enhancements demonstrate that VA's current approach is effective, aligned with risk, and meets Federal expectations.

VA also implemented strong defense-in-depth controls that significantly reduce the risk typically associated with enterprise secure configuration baseline deviations.

Key controls include the following:

- Enterprise secure configuration baseline management control leader. VA has a dedicated enterprise control leader responsible for overseeing baseline management across policy, technology, and process domains. The role ensures ongoing governance and sustained baseline compliance oversight.
- Integration of key performance indicators into enterprise monitoring [tool]. VA is incorporating key performance indicators directly into the [tool], which ties enterprise secure configuration baseline compliance to measurable, auditable performance. Enterprise secure configuration baseline compliance below [a set percentage] automatically triggers the creation of a plan of action and milestone—ensuring timely remediation and documented accountability.
- Quarterly compliance report review requirements. VA requires information security officers, or their designees, to review enterprise secure configuration baseline compliance reports quarterly, create remediation tickets in [enterprise tool], and track all outstanding issues, except for those systems which inherit enterprise-wide plans of action and milestones and are instead addressed by the appropriate managing platform support teams.
- Support for manual monitoring where automation is not possible. Where VA cannot implement automated monitoring tools (for example, certain legacy or cloud-native systems), VA requires the completion of documented manual reviews with retained evidence, which ensures continuous oversight and auditability.
- Enforced baseline deployment standards. VA enforces rigorous enterprise secure configuration baseline and hardening guides for workstations and servers through group policy objects, ensuring consistent configuration during deployment.

- Multifactor authentication enforcement for sensitive systems. Multifactor authentication mitigates credential-based attacks even in cases where baseline weaknesses may exist.
- Strict account lockout policies. These policies reduce brute force attack vectors.
- Regular vulnerability scanning. Vulnerability scanning identifies critical misconfigurations and high-severity vulnerabilities for prioritized remediation.
- Least privilege and role-based access controls. These controls restrict access pathways and limit potential impact of configuration deviations.
- Robust logging and real-time monitoring. These controls detect anomalous activity, including misuse of improperly configured systems.
- Annual security awareness training. Training mitigates human error and social engineering vulnerabilities.
- Network segmentation. This control reduces the blast radius of potential compromises resulting from misconfiguration.

VA's current practices meet Federal requirements and do not require corrective actions beyond those already in progress to achieve compliance. VA, however, is forward-looking and has plans in place to increase the security of VA's configuration management posture.

Milestones for FY 2026-29 include the following:

- Service line specific monitoring tools. These tools—targeted for implementation by September 2026—will provide full capability alignment and ensure that all platforms have reliable monitoring mechanisms.
- Policy and process updates. Planned policy and process updates will clarify expectations for identifying, reporting, and remediating misconfigurations through enterprise tools.
- Automated and manual mechanisms. Mechanisms for enhanced enterprise secure configuration baseline monitoring will ensure compliance rates of 90% or higher for all system boundaries.
- Deviation management processes. Planned processes will ensure that enterprise secure configuration baseline settings that cannot be applied are documented in system security plans with justified exceptions, consistent with Federal guidance.

Given the compensating controls and enterprise monitoring mechanisms already in place, VA assesses the residual risk associated with baseline compliance to be moderate and affirms that the Department is effectively mitigating risk.

VA remains committed to continuous improvement, enhanced automation, and active governance to ensure secure baseline implementation and compliance across the enterprise.

**Recommendation 12: 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 repeat recommendation from prior years.)***

**VA Comments:** VA non-concurs with recommendation 12. Extensive technical and administrative controls satisfy the intent of the recommendation by preventing unauthorized software. Enterprise endpoint protection, deny listing, configuration enforcement, and real-time monitoring provide strong detection and prevention capabilities across all major platforms. VA already has planned risk-based

modernization efforts in motion—including application control deployments and allow-listing strategies—which exceed the scope of the recommendation. Residual risk is demonstrably low, with no evidence indicating the need for a single automated tool.

VA operates a comprehensive, multi-layered software governance and application control program that effectively prevents the installation, execution, and persistence of unauthorized or malicious software across VA's environment. The combination of technical, administrative, and operational safeguards in place fulfills the intent of the recommendation and provides a level of protection equivalent to, or stronger than, a unified automated tool.

The extensive, layered controls already in place create a robust enterprise software management capability, even without a single unified tool.

Key controls include the following:

- Enterprise approved software restrictions. Restrictions ensure that users can only install vetted and secure applications, significantly reducing the risk of unauthorized or malicious programs.
- Deny listing, configuration logging, and centralized software approval list. These measures effectively block unauthorized execution, strengthen traceability, and improve audit readiness.
- Enterprise-grade endpoint protection. VA uses endpoint protection platforms including [specific tools] on Windows assets and [specific tool for] configuration management for Unix and Linux servers. These applications enforce least functionality principles, reduce configuration drift, and protect against malware and unauthorized changes.
- Regular vulnerability scans. Vulnerability scanning identifies malicious software. To accelerate mitigation, VA prioritizes vulnerabilities based on risk and criticality.
- Strict installation permissions. VA limits software installation permissions to trained, authorized administrators with approved access.
- Comprehensive logging and real-time monitoring. These measures detect abnormal administrative actions or suspicious execution events, reducing dwell time and improving incident response.
- Strong human-centered defensive layer. Annual security awareness training for all personnel, additional role-based training for privileged users, and clear procedural guidance and monitoring materially reduce accidental installation, social engineering risks, and administrative errors associated with software management.

VA is strengthening enterprise software governance by establishing measurable strategic milestones that exceed the scope of the recommendation. The planned initiatives progress VA toward zero trust aligned allow listing architectures.

Milestones for FY 2026-29 include the following:

- Codifying risk tolerance thresholds into policy. Policy codification will protect at least 98% of non-medical and non-special purpose Windows systems through deny listing solutions. It will also ensure that unauthorized software remains below 1% VA-wide.
- Application control deny-listing for servers and workstations. Deployment of application control deny-listing will block unauthorized and malicious applications.

- Application allow-listing for servers (planned by FY 2028) and workstations (date to be determined). Allow-listing will ensure only trusted applications can run on VA platforms.

Given the maturity of VA's technical safeguards, monitoring capabilities, endpoint tooling, and governance processes, VA assesses the residual risk associated with the lack of a single automated software management tool to be low. Existing compensating controls offer equivalent protective value and align with Federal security requirements.

VA remains committed to continuously enhancing its software asset management posture to safeguard Veteran data and maintain strong compliance with Federal cybersecurity standards.

**Recommendation 13: We recommended the Assistant Secretary for Information and Technology work with system owners to ensure adherence to established procedures for maintaining, 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.)***

**VA Comments:** VA non-concurs with recommendation 13. VA maintains strong, risk-aligned hardware and software asset management processes supported by enterprise tools, compensating controls, and strategic modernization efforts. Current VA processes provide robust inventory, monitoring, and governance—with no demonstrated systemic deficiencies. The audit results did not demonstrate systemic deficiencies or evidence that current VA practices are insufficient or that additional procedures are required beyond those already underway.

VA implemented enterprise-wide processes, governance structures, and compensating controls that address the intent of the recommendation. The capabilities already in place provide effective hardware and software inventory management, support FISMA boundary alignment, and mitigate the risks traditionally associated with incomplete or inconsistent asset inventories.

Additionally, VA maintains multiple layers of compensating and mitigating controls that significantly reduce hardware and software asset–related risks, even where full automation is still undergoing implementation. These safeguards provide both preventive and detective assurance, resulting in materially reduced risk associated with unauthorized assets or incomplete inventories.

Key controls include the following:

- Transition to the [monitoring] tool to standardize and automate asset alignment workflows and business rules; the planned completion date is April 2027. The Continuous Authorization Monitoring tool enhances accountability, accuracy, and real-time visibility over hardware asset inventory across all FISMA boundaries.
- Enterprise Software Asset Management program. VA is maturing its software asset management capabilities through the enterprise software asset management program, which implements end-to-end accountability for license-controlled software. The enterprise software asset management program provides structured processes for software intake, categorization, tracking, and lifecycle monitoring.
- Hardware Compensating Controls:
    - Automated configuration management via Puppet. Automated configuration management ensures controlled state enforcement and prevents unauthorized changes on Unix and Linux systems.

  - Real-time logging and centralized Security Information and Event Management monitoring. These controls detect anomalous changes to hardware or software assets quickly.
  - Network segmentation. This measure isolates critical systems and reduces the attack surface.
  - Vulnerability scanning. Scanning identifies unauthorized software or outdated components for prioritization and remediation.
- Software Compensating Controls:
  - Enterprise deny-list and application monitoring on Windows systems. These measures—covering approximately 90% of assets—block unapproved applications and reduce malware introduction.
  - [Specific tools]. These and other endpoint tools prevent unauthorized or malicious software execution.
  - Limited installation permissions. VA ensures only authorized, trained administrators can install software, which reduces the risk of shadow information technology.
  - Annual and role-based security training. Training reduces user error and increases awareness of safe software practices.

VA's forward-looking initiatives involve ongoing modernization. These initiatives, while further strengthening VA's enterprise-wide visibility and license management, do not reflect gaps in existing processes or deficiencies requiring remediation.

Milestones for FY 2026-29 include the following:

- Hardware inventory and asset management:
  - Automated alignment of hardware assets to FISMA boundaries. Alignment will ensure security controls and compliance reporting are accurate without manual reconciliation, reducing audit findings and resource burden.
  - Standardized business rules for asset accuracy and lifecycle tracking. Business rules will improve data quality and enable consistent decisions on refresh, decommissioning, and risk scoring across the enterprise.
- Software inventory and enterprise software asset management program:
  - Intake of all approved commercial-off-the-shelf software products. Intake will provide a single authoritative source of truth for commercial software, resulting in improved license management and security oversight.
  - Integration of cloud-provided and Government-off-the-shelf software into the central inventory. Integration will close visibility gaps, enabling full spectrum monitoring of software regardless of hosting model.
  - Inclusion of firmware and middleware in enterprise tracking. This measure will strengthen supply chain risk management by accounting for components historically overlooked but critical to security posture.
  - Policy and compliance documentation. Documentation will formalize enterprise software governance and establish enforceable standards that reduce variance, eliminate shadow information technology, and support audit readiness.

- Foundational software asset management policy and documentation. This measure will create the governance baseline required for consistent enterprise execution and future modernization.
- Cloud-provided software product intake. This action will deliver visibility into Software-as-a-Service and cloud native tools, enabling appropriate oversight, cost management, and risk assessment.
- Government-off-the-shelf software intake. This initiative will enable VA to evaluate and monitor internally developed or Government supplied software with the same rigor as commercial tools.

Given the maturity of existing safeguards and the strategic improvements already in progress, VA assesses the residual risk associated with hardware and software asset management to be moderate. VA actively manages the risk.

VA remains committed to continuous improvement and will continue enhancing asset management capabilities through continuous authorization monitoring, enterprise software asset management, and related modernization initiatives.

**Recommendation 14: 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.** ***(This is a modified repeat recommendation from prior years.)***

**Recommendation 15: 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.)***

**VA Comments:** VA non-concurs with recommendations 14 and 15. Existing enterprise Security Information and Event Management, logging, correlation, and monitoring capabilities already fulfill the intent of the recommendations. Additionally, VA is aligned with OMB M-21-31, ensuring rapid, standardized, and policy compliant incident reporting. Centralized log review is already operational in [an enterprise tool] and continues to expand. Strategic initiatives underway will further enhance visibility, detection, and enterprise-wide logging coverage beyond the scope of the recommendations.

VA operates a mature, multi-layered logging and incident response ecosystem. Existing capabilities—supported by industry standard Security Information and Event Management technologies, enterprise log aggregation, automated analytics, and centralized visibility—enable VA to detect, investigate, correlate, and respond to unauthorized or suspicious activities across the enterprise. These controls meet and, in many cases, exceed Federal expectations.

VA continues to mature its incident response and audit logging functions through capabilities that directly satisfy the objectives of the recommendations. The capabilities in place directly address improved monitoring, analysis, and centralized oversight. Additionally, VA has made enhancements that strengthen enterprise readiness, shorten detection-to-response cycles, and reinforce consistent oversight of audit related security events.

Key controls include the following:

- Industry standard Security Information and Event Management platforms. These platforms provide advanced log ingestion, correlation, and analysis across systems. The capabilities of these platforms significantly enhance VA's ability to detect unauthorized activities and unusual events.

- Central time synchronization via network time protocol. Synchronization ensures consistent event timestamps, which is essential for accurate forensic reconstruction and cross system correlation.
- Distributed logging architecture. This architecture ensures redundancy and completeness of log collection across diverse systems and platforms, reducing the likelihood of blind spots or data loss.
- Automated log analysis tools. These tools provide detection of anomalies, patterns, and threats at scale, while reducing manual effort and accelerating the identification of suspicious events.
- Cross domain correlation tools. These tools identify multi-vector or coordinated attacks that would not be detectable through siloed log review.
- Full alignment of incident response policies and processes with OMB M-21-31. Alignment to M-21-31 established capabilities for 1 hour security incident reporting through the service desk as well as standardized classification, escalation, and notification procedures.
- Consolidated enterprise audit logs and operational datasets into a centralized [enterprise tool] environment. Consolidation included [core infrastructure and security telemetry]. Consolidation improves enterprise-wide visibility, querying and threat hunting capability, incident investigation speed, cross platform correlation, and reporting and audit readiness. The capabilities of the centralized [enterprise tool] environment fulfill the requirement to centralize log review and security violation analysis across systems and platforms.

VA has planned and resourced further modernization to strengthen audit logging and monitoring beyond current levels. These strategic initiatives will eliminate remaining blind spots and further reduce the likelihood of undetected breaches.

Milestones for FY 2026-29 include the following:

- 100% visibility into bedrock, critical, and internet facing system assets at exception level 1 (September 2026).
- Full integration and centralization of disparate logging tools into a unified platform.
- Continued enhancement of automated correlation and analytics capabilities.

The combined impact of enterprise Security Information and Event Management, distributed logging, time synchronization, automated analytics, and centralized [enterprise tool] correlation reduces the likelihood of undetected unauthorized activity. Based on the layered safeguards and strong compensating controls, VA assesses the residual risk associated with audit logging and incident response to be low.

VA remains committed to continuously enhancing its cybersecurity monitoring posture and effectively capturing, analyzing, and acting upon audit events across all systems and platforms.

**Recommendation 16: 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 repeat recommendation from prior years.)***

**Recommendation 18: 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.)***

**Recommendation 19: 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. Additionally, VA should enhance their process for updating baseline images to ensure aged vulnerabilities are not introduced into the environment.** ***(This is a modified repeat recommendation from prior years.)***

**VA Comments:** VA non-concurs with recommendations 16, 18, and 19. Point-in-time scans are not a good measure of VA's continuous vulnerability management performance, policy compliance, or remediation timeliness.VA meets or exceeds all authenticated scanning thresholds, which satisfies the intent of the recommendation. VA rigorously executes remediation service level agreements, with strong evidence of timely priority 1 remediation (99% remediated or appropriately risk accepted). Mitigating strategies and compensating controls effectively address un-patchable vulnerabilities. Future risk-based initiatives exceed the scope of the recommendations and demonstrate continued program maturity.

VA employs a program of vulnerability identification, scanning, mitigation, and tracking. VA's vulnerability management program is based on risk, aligned with OMB M-20-32, *Improving Vulnerability Identification, Management, and Remediation and* NIST SP 800-53r5 and continuously executed.

The recommendations are based on point-in-time observations that do not accurately reflect the maturity, performance, or continuous operation of VA's enterprise vulnerability management program. The audit methodology relied on snapshot scans, which cannot determine how long a vulnerability existed on the network, whether VA remediate vulnerabilities within VA policy timeframes, or whether VA already mitigated vulnerabilities through a plan of action and milestones.

A vulnerability with an older [tool] publication or plugin date does not indicate the age of the vulnerability on the device, but the publication date of the detection plugin. Therefore, point-in-time scanning does not provide the most appropriate measure of policy compliance, remediation timelines, or the adequacy of VA's vulnerability management program.

VA remediates vulnerabilities on a prioritized, risk-based schedule in alignment with enterprise policy outlined in VA Handbook 6500, *Risk Management Framework for VA Information Systems VA Information Security Program*. Fiscal year-to-date performance is as follows:

- 583 priority 1 vulnerabilities identified.
- 459 remediated within 7 days.
- 80 remediated within 14 days.
- 23 remediated after 14 days.
- 5 priority 1 vulnerabilities (less than 1%) required escalation due to unique circumstances. All are on non-production, soon-to-be-decommissioned endpoints with a maintenance page applied.

VA's fiscal year-to-date performance demonstrates a highly functioning remediation process, which meets policy expectations and effectively manages outliers through proper risk acceptance and leadership oversight.

VA's enterprise scanning policy (control correlation identifier 002906) requires 75% authenticated scanning. In FY 2025, the Cybersecurity Operations Center exceeded the required threshold for every scan cycle. The results demonstrate that VA already provides adequate credentials for authenticated scanning, thereby exceeding enterprise risk tolerance thresholds.

- Over 90% authenticated scans on Windows assets.
- Over 80% authenticated scans on non-Windows assets.
- The sites OIG sampled also showed over 90% credentialed scanning success for Windows hosts.

In instances when VA cannot immediately patch or otherwise must defer vulnerabilities, VA takes appropriate mitigation measures.

VA performs vulnerability scanning of all assets every 14 days, identifying vulnerabilities as they emerge and tracking the exact date each appears on the network. Remediation service level agreements require the following mitigation timelines:

- Public facing critical risks mitigated within 15 days.
- Public facing high risks mitigated within 30 days.
- All other critical and high risks mitigated within 60 days.

VA's documented risk-based policy and operationalized enterprise tooling fully support service level agreements.

VA organizes vulnerability remediation around system authorization boundaries, each with an accountable information security officer, a designated information system security officer, and role-based remediation responsibilities enforced via VA's governance, risk, and compliance system.

The Cybersecurity Operation Center manages all enterprise scanning procedures, distributes results via the Integrated Cybersecurity Assessment, Monitoring, and Performance platform, and provides validated, authenticated data for system owner action. The governance model ensures accurate ownership, reporting, and accountability for vulnerability management. In addition, the Internal Controls Enhancement Working Group is driving continuous improvement efforts.

VA employs an array of compensating controls that strengthen vulnerability management outcomes.

Key controls include the following:

- Plans of actions and milestones. VA issued plans of action and milestones aligned to policy-driven remediation timeframes.
- Plan of Action and Milestones Vulnerability Portal. VA tracks and monitors vulnerabilities through the Plan of Action and Milestones Vulnerability Portal.
- Controls such as multifactor authentication, least privilege, intrusion detection and prevention systems, segmentation, enhanced monitoring, and application control. These controls provide effective mitigation and reduce the likelihood of exploitation.
- Manual review processes. These processes ensure coverage in environments where VA cannot use automation.
- Monthly scanning and enterprise configuration monitoring. These measures confirm that mitigations remain effective.

- Intrusion detection and prevention system network segmentation and isolation for systems requiring deferred patching.
- Enhanced logging and monitoring.
- Application control to restrict unauthorized execution.
- Manual review of systems in cases for which automated tools are not feasible.

VA is implementing initiatives for FY 2026 that further strengthen remediation timeliness and authenticated scanning.

Milestones for FY 2026 include the following:

- 70% priority 1 remediation within 7 days and 100% within 14 days and 70% within 7 days.
- More than 75% authenticated scans for all systems capable of authentication.

The controls in place significantly reduce the likelihood of exploitation of any vulnerabilities pending remediation. As a result, VA asses the residual risk to be low.

VA remains committed to protecting Veteran data and continuously strengthening enterprise vulnerability management through risk-based, measurable, and federally aligned practices.

**Recommendation 17: We recommended the Assistant Secretary for Information and Technology continue to implement controls that restrict vulnerable medical devices from unnecessary access from the general network.** ***(This is a modified repeat recommendation from prior years.)***

**VA Comments:** VA non-concurs with recommendation 17. VA isolates medical devices from the general network through access control list restricted virtual local area networks and deny-by-default communication policies. Enterprise risk assessments, monthly scanning, and plans of actions and milestones ensure continuous visibility and mitigation of vulnerabilities. VA's mature defense in-depth strategy isolates, monitors, and protects medical devices from unnecessary or unauthorized network access. This strategy provides multi-layered protection and reduces risk to an acceptable level. Future initiatives—such as zero trust aligned isolation, automation, and next generation firewall segmentation—further enhance security. Existing protections fulfill the intent of the recommendation and effectively mitigate risks associated with vulnerable medical or Internet of Medical Things devices.

VA applies multiple layers of technical and risk-based safeguards. These measures provide continuous oversight and ensure VA manages risks even when there is a lag in vendors' patch cycles.

Key controls include the following:

- Deny by default and allow by exception security model. VA maintains this model by enforcing access control lists on isolated virtual local area networks designated for medical devices. VA allows only explicitly permitted traffic to reach or originate from these virtual local area networks, substantially reducing the reachable attack surface.
- Intentional segmentation of medical devices away from the general network. Segmentation of medical devices ensures they cannot communicate with high risk or unnecessary network elements unless authorized, sharply reducing exploitation pathways and unnecessary exposure.
- Enterprise risk assessments. Before connecting any medical device to the VA isolation architecture, VA conducts an enterprise risk assessment to determine required safeguards and establish security baselines tailored to the device's risk profile. These actions ensure that VA has appropriate technical controls in place before introducing each device into the environment.

To ensure ongoing monitoring, VA performs monthly [specific tool] vulnerability scans on medical devices, tracks un-remediated vulnerabilities through plans of actions and milestones until closure. VA also applies the enterprise defense in-depth strategy, which entails multiple overlapping controls to mitigate potential vulnerabilities even before patches are available.

Medical devices benefit from VA's layered security architecture, which includes isolation virtual local area networks, access control list-based restrictions, configuration control, and enterprise security monitoring. VA's approach ensures that medical devices remain isolated, monitored, and protected. The approach ensures medical devices are not accessible or exposed to the general network. The authorizing official determined that the controls already in place reduce risk to an acceptably low level. The controls provide the necessary protection for sensitive clinical technologies.

VA is also strengthening its isolation architecture through significant strategic initiatives scheduled for FY 2026-29. Planned strategic actions demonstrate that VA is already executing a forward leaning, multi-year strategy surpassing the requirements of the recommendation.

Milestones for FY 2026-29 include the following:

- Publishing an enhanced isolation architecture aligned with zero trust principles (April 2026).
- Increasing automation of medical devices, Internet of Medical Things inventory, and vulnerability management (June 2026).
- Testing the effectiveness of enhanced vulnerability management policies for medical devices (September 2026).
- Protecting 50% of inventoried medical devices with next-generation firewall-based zone isolation, which will drastically reduce malware/ransomware blast radius (December 2026).
- Ensuring 100% of access control lists in the isolation architecture receive critical updates within 6 months of ruleset publication, which will maintain threat-aligned protection over time (December 2028).

Residual risk is low, and the controls already in place meet or exceed Federal cybersecurity requirements.

VA remains committed to protecting all medical devices and ensuring safe, secure, and uninterrupted clinical operations.

*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
Office of Accountability and Whistleblower Protection
Office of Congressional and Legislative Affairs
Office of General Counsel
Office of Information and Technology
Office of Public and Intergovernmental Affairs

## 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 vaoig.gov.**