



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 2023

Audit

23-01105-69

May 14, 2024

BE A
VOICE FOR
VETERANS

REPORT WRONGDOING
vaoig.gov/hotline | 800.488.8244

OUR MISSION

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

CONNECT WITH US



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

PRIVACY NOTICE

In addition to general privacy laws that govern release of medical information, disclosure of certain veteran health or other private information may be prohibited by various federal statutes including, but not limited to, 38 U.S.C. §§ 5701, 5705, and 7332, absent an exemption or other specified circumstances. As mandated by law, the OIG adheres to privacy and confidentiality laws and regulations protecting veteran health or other private information in this report.



DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL
WASHINGTON, DC 20001



MEMORANDUM

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

FROM: Assistant Inspector General for Audits and Evaluations

SUBJECT: VA's Federal Information Security Modernization Act (FISMA) Audit for
Fiscal Year (FY) 2023

1. Enclosed is the final report, VA's *Federal Information Security Modernization Act Audit for Fiscal Year 2023*. The VA Office of Inspector General (OIG) contracted with the independent public accounting firm CliftonLarsonAllen LLP to assess VA's information security program in accordance with FISMA.
2. To ensure the adequacy and effectiveness of information security controls, FISMA requires agency program officials, chief information officers, and inspectors general to conduct annual reviews of agencies' information security programs and report the results to the Department of Homeland Security (DHS). DHS uses these results to assist in its oversight responsibilities and prepare an annual report to Congress on agency compliance with FISMA.
3. CliftonLarsonAllen LLP is responsible for the findings and recommendations included in this report. Accordingly, the OIG does not express an opinion on VA's information security program in place during FY 2023. CliftonLarsonAllen LLP will follow up on the outstanding recommendations and evaluate the adequacy of corrective actions during its FY 2024 FISMA audit. According to findings by CliftonLarsonAllen LLP, VA continues to face significant challenges in complying with FISMA due to the nature and maturity of its information security program. Therefore, VA needs to implement improved controls. Specifically, VA should do the following:
 - Address security-related issues that contributed to the information technology material weakness reported in the FY 2023 audit of VA's consolidated financial statements.
 - Improve deployment of security patches, system upgrades, and system configurations that will mitigate significant security vulnerabilities and enforce a consistent process across all VA facilities.
 - Improve performance monitoring to ensure controls are operating as intended at all facilities, and communicate identified security deficiencies to the appropriate personnel so they can mitigate significant security risks.

4. This report provides 25 recommendations for improving VA's information security program. The FY 2022 FISMA report provided 26 recommendations for improvement. Some recommendations were modified or not closed because relevant information security control deficiencies identified during the FY 2023 FISMA audit were repeat deficiencies. One prior-year recommendation was closed because VA made significant improvements in the timely notification and resolution of computer security incidents. Despite VA's commitment to close the recommendations, some have been repeated for multiple years.
5. The effect of the open recommendations will be considered in the FY 2024 audit of VA's information security program. The OIG remains concerned that continuing delays in addressing these open recommendations could contribute to reporting a material weakness in VA's information technology security controls during the FY 2024 audit of the department's consolidated financial statements.



LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

Abbreviations

CLA	CliftonLarsonAllen LLP
DHS	Department of Homeland Security
ECSP	Enterprise Cybersecurity Strategy Program
FISMA	Federal Information Security Modernization Act
FY	fiscal year
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information and Technology
OMB	Office of Management and Budget
POA&M	Plans of Action and Milestones

May 8, 2024
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, 2023. The objective of this audit was to determine the extent to which VA's information security program and practices comply with FISMA requirements, Department of Homeland Security (DHS) reporting requirements, and applicable Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) information security guidelines. The audit included the testing of selected management, technical, and operational controls outlined in NIST's Special Publication 800-53, Revision 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 45 selected major applications and general support systems hosted at 23 VA facilities and the VA Enterprise Cloud that support the National Cemetery Administration, the Veterans Benefits Administration, and the Veterans Health Administration lines of business. Audit fieldwork occurred during the period April 2023 through October 2023.

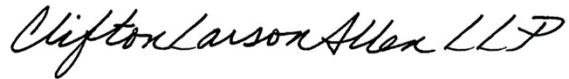
Based on our audit procedures, we concluded that VA continues to face significant challenges meeting the requirements of FISMA. This report provides 25 recommendations to assist VA in strengthening its information security program.

In connection with the audit of VA's FY 2023 Consolidated Financial Statements, we evaluated general computer and application controls for VA's major financial management systems. Significant deficiencies identified during our evaluation are included in this report. In addition to the findings and recommendations in the accompanying report, our conclusions related to VA's information security program are contained within the OMB FISMA reporting template provided to the OIG in July 2023. 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, 2023. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to October 30, 2023. The purpose of this audit report is to report on our assessment of VA's compliance with FISMA and is not suitable for any other purpose.

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

CliftonLarsonAllen LLP

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

Arlington, Virginia
May 8, 2024

Table of Contents

I. Objective	1
II. Overview	1
III. Results and Recommendations.....	2
<i>Agency-Wide Security Management Program.....</i>	<i>2</i>
<i>Identity Management and Access Controls.....</i>	<i>6</i>
<i>Configuration Management Controls</i>	<i>8</i>
<i>System Development and Change Management Controls.....</i>	<i>13</i>
<i>Contingency Planning</i>	<i>14</i>
<i>Incident Response and Monitoring</i>	<i>15</i>
<i>Continuous Monitoring</i>	<i>17</i>
<i>Contractor Systems Oversight.....</i>	<i>19</i>
Appendix A: Status of Prior Year Recommendations.....	21
Appendix B: Background	22
Appendix C: Scope and Methodology	24
Appendix D: Assistant Secretary for Information and Technology Comments.....	26
Report Distribution.....	44

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 2023 FISMA audit.

II. Overview

Information security is a high-risk area government-wide. Congress passed the Federal Information Security Modernization Act of 2014 (Public Law 113-283) in an effort to strengthen Federal information security programs and practices. FISMA provides a comprehensive framework to ensure the effectiveness of security controls over information resources that support Federal operations and assets. We assessed VA's information security program through inquiries, observations, and tests of selected controls supporting 45 major applications and general support systems at 23 VA facilities and the VA Enterprise Cloud. In FY 2023, we identified specific deficiencies in the following areas:

1. Agency-Wide Security Management Program
2. Identity Management and Access Controls
3. Configuration Management Controls
4. System Development and Change Management Controls
5. Contingency Planning
6. Incident Response and Monitoring
7. Continuous Monitoring
8. Contractor Systems Oversight

This report provides 25 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 2023 FISMA audit were repeat deficiencies. One prior year recommendation was closed because VA has made significant improvements in the timely notification and resolution of computer security incidents. Appendix A provides more details regarding the closed recommendation. The FY 2022 FISMA report provided 26 recommendations for improvement.

III. Results and Recommendations

Agency-Wide Security Management Program

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

Progress Made While Challenges Remain

In FY 2023, 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 identification, notification, and remediation of security incidents.
- Improved data quality related to background investigations and more consistent risk designations for positions across the organization.

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. VA has continued to mature its enterprise-wide risk and security management processes; however, we continue to identify deficiencies related to overall governance to include risk management processes, control assessments, Plans of Action and Milestones (POA&Ms), Authority to Operate processes, and system security plans. Each of these processes is essential for protecting VA's mission-critical systems through appropriate risk mitigation strategies and is discussed in the following sections.

Risk Management

VA has not consistently implemented components of its agency-wide information security risk management program to meet FISMA requirements. VA has established an enterprise risk management program; however, the policies, procedures, and documentation included in the program were not consistently implemented or applied across all VA systems. For example, previously known or identified system security risks were not consistently documented in corresponding remediation plans or considered in risk management decisions. Security artifacts such as Risk Assessments and POA&Ms were also not documented in accordance with VA policies. Additionally, VA's security control assessment process did not ensure that assessment teams were adequately independent from the systems under review and assessments did not address all required controls or fully evaluate the effectiveness of security controls. We also identified several instances of systems that were granted Authority to Operate without undergoing an independent assessment of security controls or having all required security documentation.

NIST Special Publication (SP) 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, states that an agency's risk management framework should address risk from an organizational perspective with the development of a comprehensive governance structure. Additionally, the Risk Management Framework requires that security control assessments are performed by groups or individuals that are free from any conflicts of interest with respect to the development, operation, or management of the information system.

VA has implemented a risk governance structure, including a Risk Management Governance Board, to monitor system security risks and implement risk mitigation controls across the enterprise. Additionally, in 2020, VA transitioned their IT systems portfolio and the associated security documentation to a new Governance, Risk and Compliance tool, entitled the Enterprise Mission Assurance Support System, to improve the process for assessing, authorizing, and monitoring the security posture of the agency. However, continued re-evaluation and shifting of VA system boundaries has complicated assignments of responsibility and ownership of system controls.

Plans of Action and Milestones

OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, defines management and reporting requirements for agency POA&Ms, to include deficiency descriptions, remediation actions, required resources, and responsible parties. According to VA's central reporting database, the department had approximately 26,197 ongoing POA&M items in FY 2023, as compared with 36,486 open POA&Ms in FY 2022. VA has dedicated additional resources to work on closing POA&Ms, but much work remains to remediate the significant number of outstanding security weaknesses. POA&Ms identify what actions must be taken to remediate system security risks and improve VA's overall information security posture.

While VA has made progress in addressing previously identified security weaknesses, we continue to identify deficiencies related to reporting, managing, and closing POA&Ms. For example, we identified: (a) POA&Ms were not consistently documented in accordance with

standards and policies, (b) POA&Ms that lacked sufficient documentation to justify closure, and (c) POA&Ms were not consistently updated to consider all known security weaknesses.

POA&M deficiencies resulted from a lack of accountability for establishing, tracking, and closing items at a “local” or “system” level and a lack of controls to ensure supporting documentation was recorded in the repository tool. System stewards and Information System Security Officers are ultimately responsible for these POA&M processes; however, they were not performing these duties in a consistent manner. By failing to fully remediate significant system security risks in the near term, VA management cannot ensure that information security controls will adequately protect VA systems throughout their life cycles. Further, without sufficient documentation in the central database to justify closure of POA&Ms, VA cannot ensure that corresponding security risks have been fully mitigated.

System Security Plans

We continue to identify system security plans with inaccurate information regarding operational environments, including control status and control implementation details that were not documented appropriately. In 2020, VA implemented a Governance, Risk, and Compliance tool to enhance their security management documentation; however, the processes and templates associated with the tool need time to mature and were not consistently documented according to VA standards. Inadequate security documentation may result in insufficient awareness and management of system risks and deficiencies as well as ineffective continuous monitoring of security controls.

CORRECTIVE ACTIONS RECOMMENDED

1. We recommended the Assistant Secretary for Information and Technology consistently implement an improved continuous monitoring program in accordance with the NIST Risk Management Framework. Specifically, implement an independent security control assessment process to evaluate the effectiveness of security controls prior to granting authorization decisions. *(This is a repeat recommendation from prior years.)*
2. We recommended the Assistant Secretary for Information and Technology implement improved mechanisms to ensure system stewards and Information System Security Officers follow procedures for establishing, tracking, and updating Plans of Action and Milestones for all known risks and weaknesses including those identified during security control assessments. *(This is a repeat recommendation from prior years.)*
3. We recommended the Assistant Secretary for Information and Technology implement controls to ensure that system stewards and responsible officials obtain appropriate documentation prior to closing Plans of Action and Milestones. *(This is a repeat recommendation from prior years.)*
4. We recommended the Assistant Secretary for Information and Technology develop mechanisms to ensure system security plans reflect current operational environments, include an accurate status of the implementation of system security controls, and all applicable security controls are properly evaluated. *(This is a repeat recommendation from prior years.)*

5. We recommended the Assistant Secretary for Information and Technology implement improved processes for reviewing and updating key security documentation, including control assessments on a risk-based rotation or as needed. Such updates will ensure all required information is included and accurately reflects the current environment. (*This is a repeat recommendation from prior years.*)

Management Comments

The Assistant Secretary for Information and Technology concurred with recommendations 1, 4, and 5 but did not concur with recommendations 2 and 3. For recommendation 1, the Assistant Secretary reported VA is implementing measures to ensure that all information systems in the authority to operate process undergo an independent control assessment during the Risk Management Framework lifecycle. This will ensure controls are successfully implemented, and control weaknesses are accurately reported as a component of the authorization package. For recommendations 4 and 5, the Assistant Secretary stated VA is taking a multi-faceted approach to ensure security documentation is accurate across all systems. This approach includes several actions for FY 2024 such as (1) updating role-based training for roles with significant system responsibilities; (2) implementing automation to auto populate key control tests directly into the Governance, Risk and Compliance tool; (3) implementing an updated and standardized authority to operate process; and (4) increasing enterprise visibility into all VA system documents and controls. For VA's non-concurrence with recommendations 2 and 3, the Assistant Secretary reported that 99 percent of all the identified Plans of Action and Milestones closures contained all appropriate documentation to close the findings and this finding does not demonstrate a pervasive issue indicative of a material weakness. Additionally, he reported VA has reduced 90 percent of ongoing Plans of Action and Milestones with an age greater than three years and has published dashboards for real-time monitoring and reporting.

OIG Contractor Response

The Assistant Secretary for Information and Technology's planned corrective actions are responsive to recommendations 1, 4, and 5. The OIG designated contractor will monitor VA's progress and follow up on implementation of the recommendations until all proposed actions are completed.

Regarding recommendations 2 and 3, both these recommendations concern POA&M process, hPlans of Action and Milestones testing was performed on 45 VA systems. For 5 of the systems tested, we identified many instances where Plans of Action and Milestones were not consistently documented with the required elements such as impact, mitigations, and recommendations. In addition, we identified several Plans of Action and Milestones that were closed with inappropriate or insufficient support to justify the remediation of the original security risk. Our testing was based on samples of closed Plans of Action and Milestones for each system and did not demonstrate a 99 percent compliance rate; contrary to management assertions. Furthermore, without sufficient documentation to justify closure of Plans of Action and Milestones, VA cannot ensure that system security risks have been fully mitigated. Accordingly, we stand by recommendations 2 and 3 that VA's processes for Plans of Action and Milestones need improvement to ensure that corrective

actions are comprehensively tracked and updated to reflect their current status. The OIG designated contractor will monitor VA's progress and follow up on implementation of the recommendations until all proposed actions are completed. Appendix D provides the full text of the Assistant Secretary's comments.

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 password management, access management, audit logging and monitoring, and personnel investigations.

Password Management

The audit team continued to identify multiple password management vulnerabilities. For example, we noted weak passwords on major databases, applications, and networking devices at many VA facilities. In addition, password parameter settings for network domains, databases, key financial applications, and servers were not consistently configured to enforce VA's password policy standards. We also identified numerous service accounts were not needed or had passwords that were not changed in over three years in accordance with VA policy. The VA Knowledge Service establishes password management standards for authenticating VA system users.

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

Access Management

Reviews of systems and permission settings identified numerous instances of unnecessary system privileges, excessive and unauthorized user accounts, accounts without formal access authorizations, and active accounts for terminated personnel. The VA Knowledge Service details access management policies and procedures for VA's information systems. Additionally, monitoring of access for individuals with elevated application privileges was lacking within several major application's production environments. This occurred because VA has not implemented effective reviews to monitor for instances of unauthorized system access or excessive permissions. Periodic reviews are critical to restrict legitimate users to specific systems and to prevent unauthorized access by both internal and external users. Unauthorized access to critical systems can leave sensitive data vulnerable to inappropriate modification or destruction.

Audit Logging and Monitoring

While VA continues to improve its centralized Security Incident and Event Management processes, we continue to identify deficiencies with how audit logs and security events are managed throughout the enterprise. Specifically, we noted that security logs were not always effectively managed, aggregated, or proactively reviewed for significant systems such as the Veterans Health Information Systems and Technology Architecture. These issues occurred because many systems and applications do not readily communicate with logging software or do not have the capability to produce comprehensive security logs. The VA Knowledge Service provides high-level policy and procedures for collection and review of system audit logs. Audit log collections and reviews are critical for evaluating security-related activities, such as determining individual accountability, reconstructing security events, detecting intruders, and identifying system performance issues. Moreover, we have identified and reported deficiencies with audit logging for more than 10 years in the annual FISMA reports.

Personnel Screening and Investigations

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

CORRECTIVE ACTIONS RECOMMENDED

6. We recommended the Assistant Secretary for Information and Technology implement improved processes to ensure compliance with VA password policy and security standards on domain controls, operating systems, databases, applications, and network devices. *(This is a repeat recommendation from prior years.)*
7. We recommended the Assistant Secretary for Information and Technology implement periodic reviews to minimize accounts and permissions in excess of required functional responsibilities, and to remove unauthorized or unnecessary accounts. *(This is a modified repeat recommendation from prior years.)*
8. We recommended the Assistant Secretary for Information and Technology enable system audit logs on all critical systems and platforms and conduct centralized reviews of security violations across the enterprise. *(This is a repeat recommendation from prior years.)*
9. We recommended the Office of Personnel Security, Human Resources, and Contract Offices implement improved processes for establishing and maintaining accurate investigation data within VA systems used for background investigations. *(This is a repeat recommendation from prior years.)*
10. We recommended the Office of Personnel Security, Human Resources, and Contract Offices strengthen processes to ensure appropriate levels of background investigations are

completed for applicable VA employees and contractors. *(This is a repeat recommendation from prior years.)*

Management Comments

The Assistant Secretary for Information and Technology concurred with recommendations 6, 7, 8, 9, and 10. For recommendation 6, the Assistant Secretary reported VA maintains 95 percent implementation of multi-factor authentication deployment throughout the environment, therefore less than 5 percent of their authentication logins in the environment use passwords. The Assistant Secretary also reported VA developed a security calendar that releases action items to the field on a periodic basis to ensure the timely maintenance of access management reviews, to include new service accounts. For recommendation 7, the Assistant Secretary reported VA has made substantial progress in addressing permission discrepancies and removing unauthorized or unnecessary accounts. For instance, VA established the Account Provisioning and Deprovisioning System to create digital identities and effectively manage identity lifecycle events. VA also updated its Identity, Credential and Access Management Directive and Handbook 6510, to align with regulatory requirements and to reflect VA's enhanced processes, procedures, and technologies. Regarding recommendation 8, the Assistant Secretary reported VA has partially mitigated the security risk of this audit logging finding by deploying an endpoint detection and resolution capability. This process allows VA to collect valuable telemetry data used to triage and investigate incidents. For recommendations 9 and 10, the Assistant Secretary reported that VA personnel security is working with VA offices involved with background investigation processes to develop or update interfaces between all systems involved to ensure enhanced data quality and consistencies between all VA (and non-VA) systems involved in the processes. For recommendations 6, 7, 8, 9, and 10, the Assistant Secretary reported additional details regarding activities to address the identified findings have been provided to the OIG contracted auditors.

OIG Contractor Response

The Assistant Secretary for Information and Technology's planned corrective actions are responsive to recommendations 6, 7, 8, 9, and 10. The OIG designated contractor will monitor VA's progress and follow up on implementation of the recommendations until all proposed actions are completed. Appendix D provides the full text of the Assistant Secretary's comments.

Configuration Management Controls

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.

Unsecure Web Applications and Services

Tests of web-based applications identified several instances of VA data facilities hosting unsecure web-based services that could allow malicious users to gain unauthorized access into VA information systems. NIST SP 800-44, Version 2, *Guidelines on Securing Public Web Servers*, recommends that organizations should implement appropriate security management practices when maintaining and operating a secure web server. Despite these guidelines, VA has not consistently implemented effective controls to identify and remediate security weaknesses on its web applications. VA has mitigated some information system security risks from the internet using network-filtering appliances. However, VA's internal network remains susceptible to attack from malicious users who could exploit vulnerabilities and gain unauthorized access to VA information systems.

While VA has implemented a 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-Frame Scripting and Session Fixation vulnerabilities was not yet formalized. Consequently, we continue to identify security vulnerabilities on web applications hosted at local facilities.

Unsecure Database Applications

While VA has made improvements in correcting database vulnerabilities, our database assessments continue to identify a number of unsecure configuration settings that could allow any database user to gain unauthorized access permissions to critical system information. NIST SP 800-160, Volume 2, Revision 1, *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, states that agencies should design, architect, and develop systems with the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises. VA has not consistently implemented effective controls to identify and remediate security weaknesses on databases hosting mission-critical applications. In addition, key VA financial management systems utilized outdated technology that hinders VA's ability to mitigate against certain information security vulnerabilities.

Application and System Software Vulnerabilities

Network vulnerability assessments identified a number of outdated operating systems and vulnerable third-party applications that could allow unauthorized access onto mission-critical systems and data. NIST SP 800-40, Revision 4 *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*, states an agency's patch and vulnerability management program should be integrated with configuration management to ensure efficiency. VA has not consistently implemented effective controls to remediate security weaknesses associated with outdated third-party applications or operating system software in a timely manner.

We also noted that many of VA's legacy systems have been obsolete for several years and are no longer supported by the vendor. Due to their age, legacy systems are more costly to maintain and difficult to update to meet existing information security requirements. Furthermore, deficiencies in VA's patch and vulnerability management program could allow malicious users to

gain unauthorized access into mission-critical systems and data. By consistently implementing a robust patch and vulnerability management program, VA could more effectively remediate vulnerabilities identified in operating systems, databases, applications, and other network devices.

Unsecure Network Access Controls

VA continued to make progress in developing access control lists to segment medical devices using the Medical Device Isolation Architecture. While extensive Access Control Lists are used to filter network communication of the general network and medical devices, we continued to identify instances where medical systems have vulnerabilities, without appropriate segmentation controls. 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 medical devices which have connectivity to otherwise segmented medical systems can expose the segmented medical devices to significant security risks that could allow malicious users to gain unauthorized access onto mission critical applications. Consequently, VA needs to strengthen its methodologies for monitoring medical devices and the trusted hosts that connect to them and ensuring they are properly segmented from other networks. Numerous critical and high-risk vulnerabilities, such as excessive system permissions, were identified on unpatched systems that support medical devices and unsecure trusted hosts that were connected to VA's general network. These insecure hosts were given the ability to access medical devices behind the Medical Device Isolation Architecture.

VA did not perform comprehensive and credentialed vulnerability scans of all systems connected to VA's network to mitigate security risks posed by these devices. Thus, VA did not have a complete inventory of existing security vulnerabilities on its networks. In addition, Office of Information and Technology (OIT) did not manage the configuration and security of certain devices in accordance with VA policy.

We also noted that several VA organizations shared the same local network at some medical centers and data centers; however, the ownership of certain devices and systems were not clearly defined for the purpose of ongoing continuous monitoring and vulnerability remediation. Consequently, some network components, not controlled by OIT, had significant vulnerabilities that weakened the overall security posture of the local facilities. VA's Enterprise Program Management Office and other offices were responsible for securing systems that are not managed by OIT. By not implementing more effective network segmentation controls for major applications and general support systems, VA is placing other critical systems at unnecessary risk of unauthorized access.

Baseline Security Configurations

VA developed guidelines to define agency-wide security configuration baselines for its major information system components. FISMA Section 3544 requires each agency to establish minimally acceptable system configuration requirements and ensure compliance. However, we noted that common platform security standards were not consistently monitored for compliance on all VA platforms. Testing also identified numerous network devices that were not configured to

a common security configuration standard, resulting in default network services, excessive permissions, weak administrator passwords, or outdated versions of system software. VA'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.

CORRECTIVE ACTIONS RECOMMENDED

11. We recommended the Assistant Secretary for Information and Technology implement more effective automated mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and web application servers. *(This is a repeat recommendation from prior years.)*
12. We recommended the Assistant Secretary for Information and Technology implement improved processes for tracking and resolving vulnerabilities that cannot be addressed within policy timeframes. Implement more effective patch and vulnerability management processes to mitigate identified security deficiencies and reduce applicable security risks. *(This is a modified repeat recommendation from prior years.)*
13. We recommended the Assistant Secretary for Information and Technology maintain a complete and accurate security baseline configuration for all platforms and ensure all baselines are appropriately monitored for compliance with established VA security standards. *(This is a repeat recommendation from prior years.)*
14. We recommended the Assistant Secretary for Information and Technology implement improved controls that restrict vulnerable medical devices from unnecessary access to the general network. *(This is a modified repeat recommendation from prior years.)*
15. We recommended the Assistant Secretary for Information and Technology enhance procedures for tracking security responsibilities for networks, devices, and components not managed by the Office of Information and Technology to ensure vulnerabilities are remediated in a timely manner. *(This is a repeat recommendation from prior years.)*
16. We recommended the Assistant Secretary for Information and Technology implement improved processes to ensure that all devices and platforms are evaluated using credentialed vulnerability assessments. *(This is a repeat recommendation from prior years.)*

Management Comments

The Assistant Secretary for Information and Technology non-concurred with recommendations 11, 12, 14, 15, and 16 but concurred with recommendation 13. For recommendations 11, 12, 15, and 16, the Assistant Secretary reported VA consistently maintains 90 percent or greater vulnerability management of all critical and high vulnerabilities across the enterprise. These statistically high percentages provide significant evidence that VA has implemented and is managing an effective Vulnerability Management and Flaw Remediation Program and aligned with industry standards. VA has established a database and web-based vulnerability tracking tool to ensure visibility, accountability, proper system owner reviews and tracking of remediation

and/or mitigation through Plans and Action and Milestones. Additionally, the Assistant Secretary reported VA made the following progress to address key areas: (1) 100 percent of systems across the environment that have priority 1 vulnerabilities have been remediated within 14 days; (2) achieved 95 percent of VA OIT managed aged critical and high vulnerabilities; (3) maintained an average of 90 percent compliance rating in addressing all critical vulnerabilities across the environment; and (4) achieved 90 percent asset alignment to system boundaries within the governance, risk and compliance tool to ensure assets are evaluated during the assessment and authorization process. For recommendation 14, the Assistant Secretary reported VA reviewed OIG findings from the Nmap discovery scans and validated the identified devices and systems were isolated and protected behind access control lists with the appropriate rules-sets as outlined in the VA Medical Device Isolation Architecture ruleset guide. The rule sets are configured to allow only minimally necessary communication ports, protocols and services for effective communications required to support the delivery of patient care.

Regarding the concurrence with recommendation 13, the Assistant Secretary stated VA OIT will develop an enterprise process for addressing security baseline deviations and ensuring appropriate mitigations are documented by September 30, 2024. For all the recommendations, the Assistant Secretary provided additional details regarding activities to address the identified findings which have been provided to the OIG contracted auditors.

OIG Contractor Response

The Assistant Secretary for Information and Technology's planned corrective actions are responsive for recommendation 13. The OIG designated contractor will monitor VA's progress and follow up on implementation of the recommendations until all proposed actions are completed.

Regarding recommendations 11, 12, 15, and 16, independent vulnerability testing was performed at all VA operated facilities. During testing, we identified numerous critical and high-risk severity vulnerabilities on networks that were due to unpatched, outdated operating systems and applications, and weak security configurations. More specifically, we continued to see older security patch issues and previously identified vulnerabilities persist on the networks. For instance, our vulnerability testing at VA's data centers revealed that the percentage of vulnerabilities over 5 years aged had not significantly changed when compared to our test results conducted during the FY 2020 FISMA audit.

For recommendation 14, we noted that network segmentation controls were in place to protect most medical devices; however, we identified several medical devices missing security updates and using operating systems and applications that were no longer supported by the vendor for security remediation. Additionally, VA's vulnerability management program did not ensure that credentialed vulnerability testing is performed on all systems across the enterprise. Thus, VA did not have a complete inventory of existing security vulnerabilities on its networks and its remediation efforts were not effective in addressing all security vulnerabilities on critical systems identified during their scanning processes. Furthermore, VA did not provide us evidence to demonstrate that: 100 percent of systems across the environment that have priority 1

vulnerabilities that have been remediated within 14 days; management has achieved 95 percent of VA OIT managed aged critical and high vulnerabilities; management has maintained an average of 90 percent compliance rating in addressing all critical vulnerabilities across the environment; and management has achieved 90 percent asset alignment to system boundaries within the governance, risk and compliance tool to ensure assets are evaluated during the assessment and authorization process. Without remediating significant security vulnerabilities on all platforms, an attacker may be able to gain unauthorized system access to modify or delete sensitive information; disrupt operations; or launch attacks against other VA systems. Accordingly, we stand by recommendations 11, 12, 14, 15, and 16 that VA's vulnerability identification and remediation processes need improvement to ensure that all significant security vulnerabilities are effectively mitigated across critical systems and platforms. The OIG designated contractor will monitor VA's progress and follow up on implementation of the recommendations until all proposed actions are completed. Appendix D provides the full text of the Assistant Secretary's comments.

System Development and Change Management Controls

VA has not consistently followed procedures to enforce standardized system development and change management controls for mission-critical systems. Consequently, we continued to identify software changes to mission-critical systems and infrastructure network devices that did not follow standardized software change control procedures.

FISMA Section 3544 requires each agency to establish policies and procedures to ensure information security is addressed throughout the life cycle of each agency information system. The VA Change Management and Knowledge Service policy also discusses integrating information security controls and privacy throughout the life cycle of each system.

Change management policies and procedures for testing and reviewing system changes were not consistently enforced for mission-critical applications and networks. We identified numerous instances of changes where testing was incomplete or missing for certain General Support Systems and major applications. VA has implemented a new change management system, which has the capability of requiring certain artifacts to be completed before changes are approved and implemented. This requirement was not in place for the legacy systems and several other applications in VA's system inventory. By not enforcing a standardized change control methodology, system development projects may be inconsistently developed, tested, and migrated into production, thereby placing VA systems at risk of unauthorized or unintended software modifications.

CORRECTIVE ACTION RECOMMENDED

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

Management Comments

The Assistant Secretary for Information and Technology non-concurred with recommendation 17 stating the OIG did not identify any site or system-level instances where changes were implemented without appropriate authorization, or any security incidents that were caused by unauthorized changes. The Assistant Secretary also reported that VA OIT achieved: (1) 95 percent of identified VA services/systems have been onboarded and are using an enterprise Information Technology Service Management tool for change control, which demonstrates an effectivity implemented change control process across the enterprise; (2) continued progress towards the key result to have less than 5 percent of major incidents caused by changes; and (3) achieved 95 percent adherence to the enterprise change control policy and standard operating procedure. The Assistant Secretary reported VA intends to deploy further change control improvements such as completing and validating configuration management plans for 100 percent critical systems. The Assistant Secretary also stated additional details regarding activities to address the identified findings have been provided to the OIG contracted auditors.

OIG Contractor Response

Regarding VA's non-concurrence with recommendation 17, configuration management testing was performed on 45 selected systems, applications, and VA geographic "area" boundaries. During testing, we identified 21 systems with inconsistent system change documentation such as test plans and test results, security impact analysis, and post-implementation verifications for the systems tested. We also noted VA does not employ automated mechanisms preventing the execution of system changes prior to approval. Consequently, individuals with appropriate access can implement changes without having formal approvals documented. We communicated these detailed change control findings within our individual site reports that were provided to management during the audit. Furthermore, VA did not provide evidence that: 95 percent of VA systems were using an enterprise Information Technology Service Management tool for change control; management continues to make progress towards the key result to have less than 5 percent of major incidents caused by changes; and management has achieved 95 percent adherence to the enterprise change control policy and standard operating procedure. Accordingly, we stand by our recommendation that VA needs to improve processes for enforcing standardized system development and change control processes that integrates security throughout the life cycle of each system. Changes made to VA systems without sufficient testing can introduce functionality defects and security vulnerabilities onto mission-critical systems. The OIG designated contractor will monitor VA's progress and follow up on implementation of the recommendations until all proposed actions are completed. Appendix D provides the full text of the Assistant Secretary's comments.

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:

- VA did not track system outages to their application boundaries and interdependent systems to accurately measure their performance against documented system recovery time objectives.
- Information system contingency plans were not consistently tested in accordance with VA policy requirements.

VA established standard recovery goals and procedures for their system boundaries but does not document which system and recovery objective is applicable when responding to outages which makes it difficult to monitor if system specific requirements were met. If business functions are not recovered within agreed upon timeframes, VA is at risk of not adequately providing mission-critical services in a consistent and resilient manner.

CORRECTIVE ACTIONS RECOMMENDED

18. We recommended the Assistant Secretary for Information and Technology implement improved procedures to ensure that system outages and disruptions are tracked to specific system boundaries and that interdependent systems are considered for the purposes of tracking and measuring against stated system recovery time objectives. *(This is a modified repeat recommendation from prior years)*
19. 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 modified repeat recommendation from prior years)*

Management Comments

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

OIG Contractor Response

The Assistant Secretary for Information and Technology's planned corrective actions are responsive to recommendations 18 and 19. The OIG designated contractor will monitor VA's progress and follow up on implementation of the recommendations until all proposed actions are completed. Appendix D provides the full text of the Assistant Secretary's comments.

Incident Response and Monitoring

Although progress has been made in relation to incident response metrics and network protections, deficiencies were noted in several areas including monitoring of network segments and monitoring of application-level security events and audit logs.

Some Internal Network Segments and Applications Not Monitored

We noted that VA's Cybersecurity Operations Center was unable to perform adequate security testing of all systems across the enterprise. Consequently, VA did not have a complete inventory of all vulnerabilities present on locally hosted systems. Ineffective monitoring of internal network segments could prevent VA from detecting and responding to intrusion attempts in a timely manner. We identified these issues at several medical facilities and data centers throughout the year. The process for tracking, updating, and reporting security-related incidents was not performed consistently throughout the year.

VA has implemented several 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 reviewed. 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.

Network Monitoring Needs Improvement

FISMA Section 3544 requires each agency to develop and implement an agency-wide information security program containing specific procedures for detecting, reporting, and responding to computer security incidents. We performed an unannounced scan of internal networks, and despite Federal requirements for detecting this type of activity, the scan was not blocked and we were not provided with evidence that a security alert was generated or incident ticket was documented. We were informed that VA's host-based solutions can produce logs of vulnerability scanning activity; however, the Cybersecurity Operations Center was still ingesting the data to actively monitor such events.

CORRECTIVE ACTIONS RECOMMENDED

20. We recommended the Assistant Secretary for Information and Technology ensure that systems and applications are adequately logged and monitored to facilitate an agency-wide awareness of information security events. *(This is a repeat recommendation from prior years.)*
21. We recommended the Assistant Secretary for Information and Technology implement improved safeguards to identify and prevent unauthorized vulnerability scans on VA networks. *(This is a repeat recommendation from prior years.)*

Management Comments

The Assistant Secretary for Information and Technology concurred with recommendation 20 and non-concurred with recommendation 21. For recommendation 20, the Assistant Secretary stated VA will work towards accomplishing the following goals: (1) 100 percent of high value assets and critical systems assets will provide telemetry data for centralized logging and monitoring; (2)

updating assessment and authorization procedures to require system owners to validate logging is enabled within their application or platform and directed to VA's enterprise logging warehouse; and (3) updating security configuration baselines with compliant logging data configuration details for systems and applications. Regarding the non-concurrence with recommendation 21, the Assistant Secretary stated the OIG's unannounced scans came from hosts that were authorized to perform scanning activities and an alert would not have been generated from a device that had already been granted approval to perform scanning activities.

OIG Contractor Response

The Assistant Secretary for Information and Technology's planned corrective actions are responsive to recommendation 20. Regarding the non-concurrence with recommendation 21, we performed several unannounced vulnerability scans that were not blocked by VA. While our scanning was authorized, management has not provided evidence of that VA is monitoring for unauthorized scanning activity such as our unannounced vulnerability testing of VA facilities outside of the scope of the FISMA audit. Accordingly, we stand by our recommendation that VA needs to improve processes for identifying and preventing unauthorized vulnerability scans on VA networks. OIT's response identified ongoing efforts to address the finding. The OIG designated contractor will monitor VA's progress and follow up on implementation of these recommendations until all proposed actions are completed. Appendix D provides the full text of the Assistant Secretary's comments.

Continuous Monitoring

Although progress has been made, VA lacks a consistent continuous monitoring program to manage agency-wide information security risks and operations. We noted deficiencies related to VA's monitoring of system security controls as well as implementing an effective patch and vulnerability management process to all devices across the enterprise. In addition, an effective agency-wide process was not fully implemented for using automation to identify 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.

Inconsistent Security Control 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. Additionally, we noted that certain security control deficiencies were not always formally tracked and reported in accordance with set policy.

Consequently, the POA&M process did not effectively communicate or track the breadth and depth of the security risks affecting mission-critical systems.

Due to inadequate monitoring procedures, our testing continued to identify significant deficiencies with configuration management controls designed to protect mission-critical systems from unauthorized access, alteration, or destruction. For instance, our testing identified unsecured web application servers, excessive permissions on database platforms, a significant number of outdated third-party applications, lack of mechanisms to prevent or detect unauthorized changes, and inconsistent platform security standards across the enterprise. We also identified devices on networks that were not incorporated into VA's overall vulnerability and patch management process. Without effectively monitoring device configurations, software, and applications installed on its networks, VA is at risk that malicious users may introduce potentially dangerous software or malware into the VA computing environment.

System Inventory Processes Need Improvement

At the time of our audit, VA had improved systems and data security control protections by enhancing the implementation of certain technological solutions, such as a central monitoring tool, secure remote access, application filtering, and portable storage device encryption. Furthermore, VA had deployed various software and configuration monitoring tools to VA facilities as part of its "Visibility to Server" and "Visibility to Desktop" initiatives and continued to implement additional tools and measures as part of the ongoing DHS Continuous Diagnostics and Mitigation program. However, VA had not fully implemented the tools necessary to compile an inventory of network components that support critical applications and program operations. Incomplete inventories of critical components could hinder VA's patch and vulnerability management processes and the restoration of critical services in the event of a system disruption or disaster.

CORRECTIVE ACTIONS RECOMMENDED

22. We recommended the Assistant Secretary for Information and Technology implement improved measures to ensure that all security controls are assessed in accordance with VA policy and that identified issues or weaknesses are adequately documented and tracked within POA&Ms. *(This is a repeat recommendation from prior years.)*
23. We recommended the Assistant Secretary for Information and Technology implement improved processes to monitor for unauthorized changes to system components and the installation of prohibited software on all agency devices and platforms. *(This is a repeat recommendation from prior years.)*
24. We recommended the Assistant Secretary for Information and Technology develop a comprehensive inventory process to identify connected hardware, software, and firmware used to support VA applications and operations. *(This is a repeat recommendation from prior years.)*

Management Comments

The Assistant Secretary for Information and Technology non-concurred with recommendation 22 but concurred with recommendations 23 and 24. For recommendation 22, the Assistant Secretary stated VA non-concurs due to the following achievements in connection with Plans of Action and Milestones findings: (1) Reducing 90 percent of ongoing Plans of Action and Milestones with an age greater than three years; (2) developing training for system stakeholders that addresses the lifecycle of Plans of Action and Milestones management; and (3) establishing a working group to provide monthly reports to provide visibility to senior executives to make risk-based decisions.

OIG Contractor Response

The Assistant Secretary for Information and Technology's planned corrective actions are responsive to recommendations 23 and 24. The OIG designated contractor will monitor VA's progress and follow up on implementation of the recommendations until all proposed actions are completed. Regarding the non-concurrence with recommendation 22, we noted that system security assessments were not performed by independent groups and certain system security deficiencies were not incorporated into VA's Plans of Action and Milestone processes. This issue was not specifically addressed in management's response to the audit report. Additionally, management did not provide us with evidence that it has reduced 90 percent of corrective actions greater than three years aged. Accordingly, we stand by our recommendation that VA needs to ensure that all security controls are assessed in accordance with VA policy and that identified weaknesses are adequately documented and tracked within Plans of Action and Milestones. The OIG designated contractor will monitor VA's progress and follow up on implementation of these recommendations until all proposed actions are completed. Appendix D provides the full text of the Assistant Secretary's comments.

Contractor Systems Oversight

VA did not fully implement contractor oversight procedures as required by FISMA. According to FISMA Section 3544, an agency should ensure adequate information security for systems that support its operations, including those provided by another agency, contractor, or other source. In addition, the VA Knowledge Service provides detailed guidance on contractor systems oversight and establishment of security requirements for all VA contracts involving sensitive VA information. Despite these requirements, our audit disclosed deficiencies in VA's contractor oversight activities in FY 2023. Specifically:

- VA did not have formal processes in place to review control assessments such as Statement on Standards for Attestation Engagements 18 reports for contractor-managed systems and ensure appropriate controls were in place. These reports provide organizations valuable information and assurances regarding the effectiveness of the service provider's control environment and VA's responsibilities not covered by the service provider.
- We identified control weaknesses on contractor-managed and operated systems such as HR Smart, Digital GI Bill, Community Care Referrals and Authorizations, and the VA Time and Attendance System.

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

CORRECTIVE ACTIONS RECOMMENDED

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

Management Comments

The Assistant Secretary for Information and Technology concurred with recommendation 25. For the recommendation, the Assistant Secretary provided additional details regarding activities to address the identified findings which have been provided to the OIG contracted auditors.

OIG Contractor Response

The Assistant Secretary for Information and Technology's planned corrective actions are responsive to recommendation 25. The OIG designated contractor will monitor VA's progress and follow up on implementation of the recommendations until all proposed actions are completed. Appendix D provides the full text of the Assistant Secretary's comments.

Appendix A: Status of Prior Year Recommendations

We noted 25 of 26 prior-year recommendations are repeated or modified and remain open within the body of this report. As noted in the table below, one recommendation was closed during the FY 2023 FISMA audit.

Table A.1. Closed Prior Year Recommendations

Number	Recommendation	Status	Corrective Actions
FISMA-2022-20	We recommended the Assistant Secretary for Information and Technology implement more effective agency-wide incident response procedures to ensure timely notification, reporting, updating, and resolution of computer security incidents in accordance with VA standards.	Closed	VA has made efforts to educate field Information System Security Officers and other personnel to ensure the timely reporting and documentation of incident tickets. We noted significant improvements in the timely notification and resolution of computer security incidents. .

Appendix B: Background

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

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

OMB and DHS provide instructions to Federal agencies and Inspectors General for preparing annual FISMA reports. In December 2022, OMB issued Memorandum M-23-03, *Fiscal Year 2023 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 2023, the metrics consisted of the core metrics and group 1 of the supplemental metrics.

The FY 2023 FISMA metrics issued by DHS established minimum and target levels of performance for these priorities, as well as metrics for other key performance areas. To comply with the reporting requirements, agencies must carry out the following activities:

- Chief Information Officers should submit monthly data through CyberScope, the FISMA reporting application. Agencies must upload data from their automated security management tools into CyberScope on a monthly basis for a specified number of data elements.
- Agencies must respond to security posture questions on a quarterly and annual basis. These questions address areas of risk and are designed to assess the implementation of security capabilities and measure their effectiveness.

- The Chief Information Officers must report to DHS on a quarterly basis, and Inspectors General and Senior Agency Officials for Privacy must report to DHS on an annual basis.
- Agencies must participate in CyberStat accountability sessions and agency interviews conducted by DHS, OMB, and the White House National Security Staff.

DHS reporting instructions also focus on performance metrics related to key control activities, such as continuous monitoring, configuration management, identity and access management, data protection and privacy, incident response, risk management, supply chain risk management, security training, and contingency planning. The OIG contracted with the independent accounting firm CliftonLarsonAllen LLP to conduct the annual FISMA audit for FY 2023. 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 45 selected major applications and general support systems hosted at 23 physical VA facilities and on the VA Enterprise Cloud that support the National Cemetery Administration, the Veterans Benefits Administration, and the Veterans Health Administration lines of business. We performed vulnerability assessments and evaluated management, operational, technical, and application controls supporting major applications and general support systems.

In connection with the audit of VA's FY 2023 Consolidated Financial Statements, CLA evaluated general computer and application controls for VA's major financial management systems, following the Government Accountability Office's *Federal Information System Controls Audit Manual* methodology. Significant financial systems deficiencies identified during CLA's evaluation are included in this report.

Site Selections

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

- VA Regional Office – Albuquerque
- VA Medical Facility – Asheville
- Information Technology Center – Austin
- VA Medical Facility – Bath
- VA Medical Facility – Biloxi
- VA Medical Facility – Charleston
- VA Medical Facility – Chicago
- Information Technology Center – Hines
- VA Medical Facility – Houston
- VA Medical Facility – Indianapolis
- VA Regional Office – Indianapolis
- Cyber Security Operations Center and Capital Region Readiness Center – Martinsburg
- Debt Management Center – Minneapolis

- Information Technology Center – Pittsburgh
- VA Medical Facility – Pittsburgh
- VA Medical Facility – San Juan
- VA Medical Facility – Sioux Falls
- VA Enterprise Cloud – Virtual
- Loan Guaranty Service – Vendor Resource Management
- VA Medical Facility – White River Junction
- VA Regional Office – White River Junction
- VA Medical Facility – Wilmington
- VA Regional Office – Wilmington

We evaluated mission-critical systems that support VA's core mission, business functions, and financial reporting capability. Vulnerability audit procedures used automated scanning tools and validation procedures to identify high-risk common security vulnerabilities affecting those mission-critical systems. In addition, vulnerability tests evaluated selected servers and workstations residing on the network infrastructure; databases hosting major applications; web application servers providing internet and intranet services; and network devices.

Government Standards

CLA conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix D: Assistant Secretary for Information and Technology Comments

Department of Veterans Affairs Memorandum

Date: February 1, 2024

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

Subj: Office of Inspector General Draft Report, VA's Federal Information Security Modernization Act Audit for Fiscal Year 2023 (VIEWS 11246793)

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

1. Thank you for the opportunity to comment on the Office of Inspector General (OIG) draft report, Federal Information Security Modernization Act Audit for Fiscal Year 2022.
2. The report provides 25 recommendations for improving the Department's information security program. The Office of Information and Technology (OIT) submits written comments to the recommendations, including strategic responses and accomplishments and remediation goals.

<i>The OIG removed point of contact information prior to publication.</i>

(Original signed by)

Kurt D. DelBene

Attachment
Office of Information and Technology
Comments to Office of Inspector General Draft Report,
Federal Information Security Modernization Act Audit for Fiscal Year 2023
(VIEWS 11246793)

Fiscal Year (FY) 2023 Federal Information Security Modernization Act Audit (FISMA) Response Summary

Thank you for the opportunity to review the Office of Inspector General (OIG) report, Federal Information Security Modernization Act Audit for Fiscal Year 2023. This report provides valuable insight into the status of our organization's security control compliance, and we appreciate the continued partnership with the OIG's security audit team. Our teams' partnership to review these controls during the audit cycle highlights the Department of Veterans Affairs (VA) Office of Information and Technology's (OIT) commitment and dedication toward security excellence.

In FY 2023, VA OIT made significant strides in pursuing strategic goals with a risk-based approach to protecting Veteran data and ensuring the confidentiality, integrity and availability of essential services for our Veterans. Our remediation plans, in turn, focus on those vulnerabilities which are most critical to VA based on our knowledge of the infrastructure and systems we oversee. As a direct result of these continued efforts and year-over-year advances, there has been a demonstrable improvement in VA's security posture. This year, we successfully closed two FY 2022 findings related to contingency planning. Moreover, VA persisted in preventing findings related to memoranda of understanding/interconnection security agreements and external connections, demonstrating resiliency and maturity in these controls.

VA also significantly strengthened cybersecurity throughout FY 2023 in the following areas:

VA resolved all enterprise baseline compliance monitoring discrepancies within BigFix, which resulted in increased accuracy of compliance monitoring.

Through VA's application control initiative, VA implemented a deny list (blacklist) approach for prohibited software instances on client operating systems. The usage of a deny list significantly restricts the ability of VA users to use prohibited software on agency devices and platforms. The installation of software within the VA environment is limited to users with administrative rights and/or enterprise-approved applications.

By assigning system boundaries in our governance, risk and compliance (GRC) tool, VA enabled system ownership accountability and increased visibility. VA established a process to identify network-connected assets by system boundary using our existing GRC tool. Each system boundary contains an identified, accountable system owner who is responsible for managing associated assets and their vulnerabilities.

VA achieved a target of 94% deployment of endpoint detection capabilities (77% endpoint detection and resolution [EDR] and 17% mobile threat defense [MTD]), which enhances the enterprise security visibility across the enterprise.

Rather than conducting a comprehensive, risk-based assessment of VA's security posture, the annual OIG FISMA audit focuses primarily on assessing the implementation and effectiveness of VA's security policies as implemented through our security controls. As such, it does not take into consideration the degree of risk posed by identified deficiencies. It does not consider VA's own risk-based assessment of our broad, complex environment and the cybersecurity goals that result from this assessment. As a result, relatively lower priority issues may be flagged as indicating a significant security gap. The assessment may also fail to recognize progress made and incorrectly identify issues. For example, the

recommendation related to change management indicates VA does not have a process in place for change control. However, VA has a very robust enterprise-level policy and process in place for change control. While we acknowledge that opportunities remain for improvement of system-level compliance with policy, processes and the Information Technology Service Management Tool (ITSM), this is not the issue OIG identified.

Another challenge caused by the audit approach is the limited detail that accompanies the findings. This degrades VA's ability to analyze findings, understand the operational causes and target effective remediations based on relative risk. Through analysis of the findings, VA OIT has noted inconsistencies in reporting, such as total sample size is frequently not identified. Additionally, Recommendation 23 prescribes improving the monitoring of prohibited software installations on the network; however, VA performance metrics demonstrate a strong capability that blocked 22,879 prohibited software executions over a nine-month period. OIG did not provide any findings across the 45 audited system boundaries that referenced prohibited software instances, or software instances installed without authorization. This lack of relevant data concerning the findings not only decreases the remediation accuracy and efficiency, but also places an administrative burden of analyzing, handling and tracking multi-system/multi-control composite findings on VA staff. VA OIT would like to see OIG implement a standardized template that would require separate findings to be written for each information system boundary and FISMA security control.

It is also important to note that while the annual FISMA audit provides valuable insight into the performance of VA's security controls, it is only one of many approaches VA uses to assess and mitigate risk. Consequently, there is not a complete alignment between VA's risk-based priorities and OIG's compliance-based audit findings, as compliance does not necessarily equate to an improved security posture. For example, the OIG cites VA for not deactivating accounts that are inactive over 90-days, which is current VA policy.

Ultimately, VA appreciates the independent insights afforded by the annual FISMA audit and is excited to see demonstrable enterprise progress in the remediation of long-standing security deficiencies reflected in this year's audit report. VA will continue to resolve identified security deficiencies and align with broader organizational cybersecurity strategies in the coming years. In support of this, VA OIT developed practical and measurable targets for FY 2024 (attached within the written comments) as we continue to strive to meet our strategic goals.

Office of Information and Technology
Comments on Office of Inspector General Draft Report,
Federal Information Security Modernization Act Audit for Fiscal Year 2023
(VIEWS 11246793)

OIG FISMA Recommendations 1, 4 and 5

Notices of Findings and Recommendations (NFR) Number: 1.01-1.03

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

Recommendation 4: We recommended the Assistant Secretary for Information and Technology develop mechanisms to ensure system security plans reflect current operational environments, include an accurate status of the implementation of system security controls, and all applicable security controls are properly evaluated.

Recommendation 5: We recommended the Assistant Secretary for Information and Technology implement improved processes for reviewing and updating key security documentation, including control assessments on a risk-based rotation, or as needed. Such updates will ensure all required information is included and accurately reflects the current environment.

Comments: Concur.

Strategic Response and Accomplishments:

VA concurs with findings for the information security program and has identified remediation efforts for these findings. These efforts include training security control assessment stakeholders to 1) properly complete security documentation and 2) track periodic action items requiring the review and completion of system security documentation, all of which will facilitate accountability for stakeholders.

VA is implementing measures to ensure that all information systems in the authority to operate (ATO) process undergo an independent control assessment while in Step 4 of the RMF lifecycle. This will ensure that controls are successfully implemented, and control weaknesses are accurately reported as a component of the authorization package. VA is taking a risk-based approach for security control assessments (SCA) by conducting SCAs against critical systems and high-value assets (HVA) in FY 2024.

VA is taking a multi-faceted approach to ensure security documentation is accurate across all systems. This approach includes the following actions for FY 2024:

- Updating role-based training for roles with significant system responsibilities.
- Implementing automation to auto populate key control tests directly into the GRC tool.
- Implementing an updated and standardized ATO process.
- Increasing enterprise visibility into all VA system documents and controls.

In FY 2023, VA implemented the following actions to address the recommendations:

- Developed a security calendar that releases action items to the field on a periodic basis to ensure timely maintenance of key security documentation.

- Integrated VA System Inventory and GRC tool registration processes to avoid duplication of legacy data. VA can now track real-time system level efforts for one-to-one mapping via a dashboard.
- Deployed an annual self-assessment review capability within the GRC tool for stakeholder validation, document test evidence and implement an accountability structure for system security activity approvals.

Remediation Goals:

By October 2025, VA will complete the below to resolve identified information security management material weakness:

- 100% of critical systems undergoing ATOs will have an independent security assessment by September 30, 2024.
- 100% of key security documentation will be current and accurate for critical systems undergoing ATOs by September 30, 2024.
- 100% of all FISMA reportable systems will achieve a current and accurate population of key security documentation by September 30, 2025.
- 100% of FISMA reportable systems undergoing an ATO will have an independent security assessment by October 1, 2025.

OIG FISMA Recommendations 2, 3 and 22

NFR: 5.01-5.02

Recommendation 2: We recommended the Assistant Secretary for Information and Technology implement improved mechanisms to ensure system stewards and Information System Security Officers follow procedures for establishing, tracking, and updating Plans of Action and Milestones for all known risks and weaknesses including those identified during security control assessments.

Recommendation 3: We recommended the Assistant Secretary for Information and Technology implement controls to ensure that system stewards and responsible officials obtain appropriate documentation prior to closing Plans of Action and Milestones (POA&M).

Recommendation 22: We recommended the Assistant Secretary for Information and Technology implement improved measures to ensure that all security controls are assessed in accordance with VA policy and that identified issues or weaknesses are adequately documented and tracked within POA&Ms.

Comments: Non-concur.

Strategic Response and Accomplishments:

VA non-concurs with Recommendations 2, 3, and 22. Per the FY 2023 FISMA audit, 99% of POA&M closures contained all appropriate documentation to close findings; this finding does not demonstrate a pervasive issue indicative of a material weakness.

In FY 2023, VA achieved the following to aid in remediation of POA&M findings:

- Reduced 90% of ongoing POA&Ms with an age greater than three years.
- Developed training for system stakeholders that addresses the lifecycle of POA&M management.

- Published POA&M dashboards for real-time monitoring and reporting.
- Established the POA&M working group (WG) to provide monthly reports to achieve the following:
 - Escalation of trigger points into the enterprise risk registry that provides visibility to senior executives to make risk-based decisions.
 - Serves as an enforcement mechanism to hold system stakeholders accountable for the timeliness, accuracy and sufficiency of their systems' POA&Ms.

Remediation Goals:

By September 30, 2024, OIT's continuous monitoring program will accomplish the following:

- 90% reduction in reported non-compliant security controls without an associated POA&M.

OIG FISMA Recommendation 6

NFR: 7

Recommendation 6: We recommended the Assistant Secretary for Information and Technology implement improved processes to ensure compliance with VA password policy and security standards on domain controls, operating systems, databases, applications, and network devices.

Comments: Concur.

Strategic Response and Accomplishments:

VA concurs with OIG's findings and recommendations concerning improving password policy and secure configuration standards. VA maintains 95% implementation of multi-factor authentication deployment throughout the environment, therefore less than 5% of our authentication logins in the environment use passwords. VA has deployed a privileged access management system for administrator and service accounts.

While VA concurs with identified findings, the analysis of these findings does not demonstrate widespread failure of controls of service accounts. VA has demonstrated a significant level of maturity in access management of service accounts:

- 76% of the systems reviewed by OIG had no service account password findings.
- 93% of the systems reviewed by OIG had no service account review findings.
- 76% of the systems reviewed by OIG had no inactive service account findings.
- 87% of the systems reviewed by OIG had no findings with justifications for the service accounts.

In alignment with VA's Zero Trust First Cybersecurity Strategy, VA has achieved greater visibility, improved reporting and deployed the privileged access management to secure service accounts.

The following tasks were performed in FY 2023 to aid in remediation of the enterprise-level weaknesses identified with VA password policy:

- Developed a security calendar that releases action items to the field on a periodic basis to ensure timely maintenance of access management reviews.
- Onboarded all new service accounts into the privileged access management system.

Remediation Goals:

By May 2024, VA will complete work towards the following key results to address the residual risk related to remaining system-level change control deficiencies:

- 100% of service accounts with interactive logon enabled will have passwords changed every 60 days by May 31, 2024.

OIG FISMA Recommendation 7

NFR: 4

Recommendation 7: We recommended the Assistant Secretary for Information and Technology implement periodic reviews to minimize accounts and permissions in excess of required functional responsibilities, and to remove unauthorized or unnecessary accounts.

Comments: Concur.

Strategic Response and Accomplishments:

VA concurs with OIG's findings and recommendations related to periodic reviews needed to minimize account and permission discrepancies and to remove unauthorized or unnecessary accounts. The number of issues reported indicate a significant level of maturity in access management practices across the enterprise. Below are points of clarification VA OIT would like to highlight regarding OIG's findings:

Access Reviews:

- 71% of the systems reviewed by OIG had no findings with user access reviews. Of the 5,138 identified accounts, 99% were found within one system.
- 71% of the systems reviewed by OIG had no findings with disablement of inactive accounts. Of the 9,265 accounts, 91% were found within one system.

Access Approvals:

- 76% of the systems reviewed by OIG had no findings with user access approvals or where evidence of approvals was not provided. Of the 167 identified accounts, 48% were found within one system.

Separation Checklist:

- 76% of the systems reviewed by OIG had no findings with user separation. Of the 79 identified accounts, 65% were found within three systems.

Elevated Privilege Account Monitoring:

- 82% of the systems reviewed by OIG had no findings with approvals for privileged access. Of the 51 identified accounts, 73% were within three systems.
- 91% of the systems reviewed by OIG had no findings with inactive accounts with privileged access. Of the 2,691 identified accounts, 99% were found within one system.
- 82% of the systems reviewed by OIG had no findings with review of accounts with privileged access.

VA OIT achieved many strategic accomplishments and made substantial progress in addressing key areas to support implementation of the recommendations:

- Established the Account Provisioning and Deprovisioning System (APDS) to create digital identities and effectively manage identity lifecycle events. This system acts as a single repository to effectively govern all VA user identities.
- Updated VA's Identity, Credential and Access Management (ICAM) Directive and Handbook 6510, to align VA policy to released regulatory requirements and to reflect VA's enhanced ICAM processes, procedures and technologies. Policy publication and implementation is scheduled for FY 2024.

Remediation Goals:

VA will complete the below to resolve the identified access control findings:

- Establish, adopt and enroll 100% of enterprise users into a solution that will serve as a central point to manage separation of duties, establish periodic access reviews of both privileged and non-privileged accounts, validate that user access request forms are completed and authorized in accordance with policy and enhance workforce user identity lifecycle management. This effort is scheduled to be completed by December 31, 2025.
- Manage 100% of the VA workforce (approximately 624,000 personnel) in VA's enterprise-wide solution to provide a centralized and standardized process for monitoring contractors, employees, volunteers, Health Professional Trainees Without Compensation (HPT/WOC) and accredited representatives/affiliates access. The centralization of this solution will support user access being timely and properly deprovisioned upon termination or position change.
 - 100% of contractors managed in APDS by March 31, 2024.
 - 100% of HPT/WOCs managed in APDS by March 31, 2024.
 - 100% of volunteers managed in APDS by July 31, 2024.
 - 100% of employees managed in APDS by October 31, 2024.
 - 100% of accredited representatives/affiliates managed in APDS upon completion of functionality.

OIG FISMA Recommendations 8 and 20

NFR: 8

Recommendation 8: We recommended the Assistant Secretary for Information and Technology enable system audit logs on all critical systems and platforms and conduct centralized reviews of security violations across the enterprise.

Recommendation 20: We recommended the Assistant Secretary for Information and Technology ensure that systems and applications are adequately logged and monitored to facilitate an agency-wide awareness of information security events.

Comments: Concur.

Strategic Response and Accomplishments:

VA concurs with OIG's conclusions and recommendations regarding logging and security events. VA has partially mitigated the security risk of this finding through an EDR capability deployed to 737,879 endpoints (77% EDR and 17% MTD). EDR allows VA to collect valuable telemetry data used to triage and investigate incidents.

VA has taken a risk-based approach in addressing Office of Management and Budget (OMB) M-21-31 requirements and prioritized the completion of logging and monitoring our most critical systems by the end of FY 2024. Due to size, scope and complexity of VA's environment, VA has projected a significant shortfall in resources to achieve full compliance with M-21-31.

- 74% of HVA systems are compliant in meeting event logging (EL) 1 and EL2 requirements and projected to meet EL3 maturity for HVA systems by December 31, 2024.

Remediation Goals:

By FY 2024, VA will work towards accomplishing the following key performance goals:

- 100% of HVA, bedrock and critical systems assets provide telemetry data for centralized logging and monitoring.
- Update assessment and authorization (A&A) procedures to require system owners to validate logging is enabled within their application or platform and directed to VA's enterprise logging warehouse.
- Update security configuration baselines with compliant logging data configuration details for systems and applications.

OIG FISMA Recommendations 9 and 10

NFR: 2

Recommendation 9: 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.

Recommendation 10: We recommended the Office of Personnel Security, Human Resources, and Contract Offices strengthen processes to ensure appropriate levels of background investigations are completed for applicable VA employees and contractors.

Comments: Concur.

Strategic Response and Accomplishments:

VA concurs with Recommendations 9 and 10, where OIG found instances of data quality issues and inconsistencies across HR SMART, VA Centralized Adjudication Background Investigation System (VA-CABS) and other systems involved with background investigation processes.

VA personnel security is working with VA offices involved with background investigation processes to develop or update interfaces between all systems involved to ensure enhanced data quality and consistencies between all VA (and non-VA) systems involved in the processes. The Center for Enterprise Human Resources Information Services program is developing and updating human capital information systems (HCIS) to ensure enhanced data quality and consistencies between eClass360/HR SMART. Change Request (CR) 343 completes the interconnection between eClass360, VA's automated classification system and HR SMART. The interconnection will transmit the position sensitivity, position risk, and investigation level determined by trusted workforce standards. This data will not be editable in HR SMART. Modifications will need to be made in eClass360 and re-transmitted to HR SMART. HR SMART will document on a user dashboard when changes are received and will alert position manager's that a change has been detected which requires action. The subsequent audit workflow and dashboard will ensure system users are alerted to incongruencies and when appropriate action is required. The CR 343 is expected to be completed FY 2024 Q3.

Human Resources and Administration/Operations, Security and Preparedness (HRA/OSP) is working to take the corrective actions listed above. HRA/OSP has implemented improved processes for establishing and maintaining accurate investigation data by leading the NFR 2 IPT, which brought VA stakeholders together to tackle the NFR 2 recommendations from FY 2022 NFR findings. The result of the NFR 2 IPT was the VA-CABS Data and Interface WG and HR-Smart Data and Interface WG.

HRA is leading the HR-Smart Data and Interface WG, which is working to update the HCIS to ensure enhanced data quality and consistencies between eClass360/HR SMART. An upcoming update to HR SMART will complete the interconnection between eClass360, VA's automated classification system, and HR SMART. HR SMART will be updated regularly by eClass360 when modifications are made to position designation, as eClass360 is the system of record for position designation. A key recommendation has been made by the WG to discontinue updating background investigation data in HR SMART. In 2022, the system of record notice was issued for VA-CABS, making VA-CABS the system of record, so background investigation data should only be stored in VA-CABS. Removal of background investigation data from HR SMART will help remediate inconsistent data findings.

HRA/OSP is leading the VA-CABS Data and Interface WG which conducted a VA-CABS data cleanup, using the position risk matrix as a guide to review 100% of VA-CABS' employee position designation data. By conducting this review, HRA/OSP was able to identify incorrect employee position data in VA-CABS to establish what the correct level of background investigation should be for employees. The position risk matrix also allowed for remediation of incorrect position designations in VA-CABS, correcting over 10,000 incorrect position designations. VA-CABS 2.0 was launched in FY 2023 and features improved data quality and reporting capabilities. Personnel security continues to work on improvements to contractor, HPT and other staff (WOCs, affiliates, volunteers, etc.) data in FY 2024.

In FY 2023, personnel security developed the VA-CABS personnel security data system requirements document, which identifies needed system improvements for VA-CABS 2.0, including interoperability connections with other systems, including APDS. Personnel security will work with VA OIT to pursue development of these requirements in FY 2024.

HRA/OSP personnel security remediated over 80% of the position risk designation data in VA-CABS for all employees. From that effort, the final percentage of employees with compliant position designations exceeded the 95% threshold.

Remediation Goals

By December 31, 2024, VA will complete work towards the following key results to resolve the identified material weakness:

- 95% of position risk designation data is updated and validated as accurate for all employees in HR-SMART by date to be determined.
- 95% of position risk designation data is updated and validated as accurate in VA-CABS for all employees by December 31, 2024.
- 95% of position risk designation data is updated and validated as accurate in VA-CABS for contractors by December 31, 2024.
- 95% of position risk designation data is updated and validated as accurate in VA-CABS for HPTs by December 31, 2024.
- 95% of position risk designation data is updated and validated as accurate in VA-CABS for all other staff (WOCs, affiliates, volunteers, etc.) by December 31, 2024.

- 95% of fingerprint and background investigation records in VA-CABS are updated and accurate, for all employees by February 29, 2024.
- 95% of fingerprint and background investigation records in VA-CABS are updated and accurate for all contractors by December 31, 2024.
- 95% of fingerprint and background investigation records in VA-CABS are updated and accurate, for all HPTs by December 31, 2024.
- 95% of fingerprint and background investigation records in VA-CABS are updated and accurate, for all other staff (WOCs, affiliates, volunteers, etc.) by December 31, 2024.

OIG FISMA Recommendations 11, 12, 15, and 16

NFR: 9.01; 9.04-9.05

Recommendation 11: We recommended the Assistant Secretary for Information and Technology implement more effective automated mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and web application servers.

Recommendation 12: We recommended the Assistant Secretary for Information and Technology implement improved processes for tracking and resolving vulnerabilities that cannot be addressed within policy timeframes. Implement more effective patch and vulnerability management processes to mitigate identified security deficiencies and reduce applicable security risks.

Recommendation 15: We recommended the Assistant Secretary for Information and Technology enhance procedures for tracking security responsibilities for networks, devices, and components not managed by the Office of Information and Technology to ensure vulnerabilities are remediated in a timely manner.

Recommendation 16: We recommended the Assistant Secretary for Information and Technology implement improved processes to ensure that all devices and platforms are evaluated using credentialed vulnerability assessments.

Comments: Non-concur.

Strategic Response and Accomplishments:

VA non-concurs with these recommendations and has addressed OIG's concerns as part of the FY 2023 improvements and continues to mature our vulnerability management processes as part of the vulnerability management lifecycle.

VA consistently maintains 90% or greater vulnerability management of all critical and high vulnerabilities across the enterprise. These statistically high percentages provide significant evidence that VA has implemented and is managing an effective Vulnerability Management and Flaw Remediation Program and aligned with industry standards. VA has established a database and web-based vulnerability tracking tool to ensure visibility, accountability, proper system owner reviews and tracking of remediation and/or mitigation through POA&Ms. VA also uses a risk-based approach to address detected vulnerabilities with a prioritized status. A combination of an asset's business impact, likelihood of vulnerability exploitation, and exposure of the asset to the adversary (e.g., internet facing) are used to prioritize remediation actions.

OIG reported that unannounced vulnerability scans were not blocked by VA. The unannounced scans came from hosts that were authorized to perform scanning activities. As a part of audit practices, an alert would not have been generated from a device that had already been granted approval to perform scanning activities.

VA has made the following progress in FY 2023 to address key areas to support resolution of this recommendation:

- 100% of systems across the environment that have priority 1 vulnerabilities have been remediated within 14 days.
- Achieved 95% of VA OIT managed aged critical and high vulnerabilities (against October 2022, FY 2023 baseline).
- Maintained an average of 90% compliance rating in addressing all critical vulnerabilities across the environment.
- Achieved 90% asset alignment to system boundaries within the GRC tool to ensure assets are evaluated during the A&A process. The A&A process requires the use of credentialed vulnerability assessments in obtaining an ATO.
- Implemented end-of-life (EOL) procedures ensuring that existing EOL platforms and applications are remediated via decommission plans and POA&Ms.

Remediation Goals:

Not applicable.

OIG FISMA Recommendation 13

NFR: 6.03

Recommendation 13: We recommended the Assistant Secretary for Information and Technology maintain a complete and accurate security baseline configuration for all platforms and ensure all baselines are appropriately monitored for compliance with established VA security standards.

Comments: Concur.

Strategic Response and Accomplishments:

VA concurs with Recommendation 13 to maintain a complete and accurate security baseline configuration for all platforms and ensure all baselines are appropriately monitored for compliance with established VA security standards.

In FY 2023, VA maintained an authoritative repository of enterprise-level baselines and corrected monitoring deficiencies to reflect process gaps.

Remediation Goals:

VA OIT will develop an enterprise process in addressing security baseline deviations and ensuring appropriate mitigations are documented by September 30, 2024.

OIG FISMA Recommendation 14

NFR: 9.02

Recommendation 14: We recommended the Assistant Secretary for Information and Technology implement improved controls that restrict vulnerable medical devices from unnecessary access to the general network.

Comments: Non-concur.

Strategic Response and Accomplishments:

VA non-concurs that improved controls are needed to restrict vulnerable medical devices from unnecessary access to the general network. VA reviewed OIG findings from the Nmap discovery scans (subset sampling of OIG IPs) and validated the identified devices and systems were isolated and protected behind access control lists (ACL) with the appropriate rules-sets for communication management. As outlined in the VA Medical Device Isolation Architecture ruleset guide, ACLs are designed to “Deny by Default” and “Allow by Exception” for network communication “To” and “From” the isolated virtual local area network.

The medical device program conducts security evaluations that are assessed for impact analysis and approved through the Configuration Control Board. The ACLs are configured to allow only minimally necessary communication ports, protocols and services for effective communications required to support the delivery of patient care. In addition, VA maintains scripting that provides automated continuous ACL configuration compliance checks based on daily ACL configuration collections across the enterprise.

VA isolation architectures with implemented ACLs effectively mitigate and reduce the likelihood of exploitations and minimizes the security risk to VA to an acceptable level as authorized and approved by the Authorizing Official.

Remediation Goals:

In FY 2024, VA will complete the following to further improve the security of medical devices:

- As VA continues its rollout of the Electronic Health Record (EHR) to VA medical centers, the medical devices will be placed behind firewalls in the medical zone architecture. This process is ongoing to match the EHR Modernization rollout schedule.
- ACL vulnerability and remediation trends and compliance will be made visible.

OIG FISMA Recommendation 17

NFR: 6.01-6.02

Recommendation 17: We recommended the Assistant Secretary for Information and Technology implement improved procedures to enforce standardized system development and change control processes that integrates information security throughout the life cycle of each system.

Comments: Non-Concur.

Strategic Response and Accomplishments:

VA non-concurs with Recommendation 17 to implement improved procedures to enforce standardized system development and control processes that integrate information security throughout the life cycle of systems. OIG did not identify any site or system-level instances where changes were implemented without appropriate authorization, or any security incidents that were caused by unauthorized changes. VA OIT has a mature enterprise change control policy, a supporting standard operating procedure and work instructions detailing appropriate implementation.

Enhancements made throughout FY 2022 into FY 2023 include:

- Change control forms to provide testing consistency, and onboarding of VA financial systems to the change control program.
- Systems that do not adhere to enterprise change control policies and procedures are captured in POA&M items within each information system security plan. In accordance with the POA&M items, VA OIT system owners are actively working remediation efforts based on criticality and assessed risk for each system.

- Updated VA Directive 6004, approved in January 2023, establishes and maintains OIT-wide configuration, change and release management programs in accordance NIST SP 800-128.
- VA established and disseminated written work instructions on managing unauthorized emergency change requests, and implemented a change control probation process where stakeholders that continuously do not abide by change manage procedures have their change provider permissions revoked.
- The major incident management process performs reviews on major incidents caused by change, and they conduct a post-implementation review. The implementation of this process as a detective control function for VA increases oversight and accountability of unauthorized changes.

In FY 2023, VA OIT has achieved the following:

- 95% of identified VA OIT services/systems have been onboarded and are using enterprise ITSM for change control, which demonstrates an effectivity implemented change control process across the enterprise.
- VA OIT continues to make progress towards the key result to have less than 5% of major incidents caused by changes.
- VA OIT has achieved 95% adherence to the enterprise change control policy (VA Directive 6004) and standard operating procedure.

Remediation Goals:

In FY 2024, VA intends to deploy the following to further improve change controls:

- 100% of critical systems have complete and validated configuration management plans uploaded to GRC tool within the last year.

OIG FISMA Recommendations 18 and 19

NFR: 3

Recommendation 18: We recommended the Assistant Secretary for Information and Technology implement improved procedures to ensure that system outages and disruptions are tracked to specific system boundaries and that interdependent systems are considered for the purposes of tracking and measuring against stated system recovery time objectives.

Recommendation 19: 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.

Comments: Concur.

Strategic Response and Accomplishments:

VA concurs with OIG's findings and recommendations regarding contingency planning. VA has prepared systems to be compliant with contingency planning by establishing standardized, automated templates for Business Impact Analysis (BIA), Information System Contingency Plan (ISCP) and Disaster Recovery Plan (DRP), available through the centralized Knowledge Service.

In FY 2023, VA OIT achieved the following tasks to aid in remediation of contingency planning material weaknesses:

- Updated Handbook 6500.8 and contingency planning controls to align with NIST and federal guidance.
- Developed training and exercise materials resulting in increased knowledge among key stakeholders in contingency planning operations.

Remediation Goals:

In FY 2024, VA will complete work towards the following key results to resolve the identified contingency planning material weaknesses:

- Update VA Handbook 6500.8 to correct over 300 elements that required updating to ensure information systems are compliant with established thresholds for HVA systems, high impact systems and moderate or low impact systems. This policy will ensure that artifacts are current and meet contingency procedures.
- VA will develop contingency planning policy in VA Handbook 6500.8 that establishes requirements and guidelines on planning, recovery time objectives and testing of contingency plans; and submit the policy in VA Integrated Enterprise Workflows System for concurrence and approval by September 30, 2024.
- VA will establish standardized and automated templates for BIA, ISCP and DRP development to ensure completion of required data fields and necessary planning efforts by December 18, 2024.
- VA OIT is 80% complete with a project to align security system boundary to operations service maps, and products. Once complete VA OIT will maintain a 1:1:1 relationship with system boundary. The completion of this project will allow VA OIT to ensure system outages are aligned to specific system boundaries and their recovery time objectives.

OIG FISMA Recommendation 21

NFR: 8

Recommendation 21: We recommended the Assistant Secretary for Information and Technology implement improved safeguards to identify and prevent unauthorized vulnerability scans on VA networks.

Comments: Non-concur.

Strategic Response and Accomplishments:

VA non-concurs with Recommendation 21. OIG reported that unannounced vulnerability scans were not blocked by VA. The unannounced scans came from hosts that were authorized to perform scanning activities. As a part of audit practices, an alert would not have been generated from a device that had already been granted approval to perform scanning activities.

OIG stated they performed unannounced vulnerability scans that were not blocked by VA, but their testing methodology was not valid. In practice, the OIG performed a scan of an adjacent facility – one that was not included in their authorized audit – thinking this would generate an alert. However, these unannounced scans came from hosts that were authorized to perform scanning activities, regardless of what facility they were scanning. An alert would not have been generated from a device that had already been granted approval to perform scanning activities.

Remediation Goals:

Not applicable.

OIG FISMA Recommendation 23

NFR: 6.04

Recommendation 23: We recommended the Assistant Secretary for Information and Technology implement improved processes to monitor for unauthorized changes to system components and the installation of prohibited software on all agency devices and platforms.

Comments: Concur

Strategic Response and Accomplishments:

VA concurs with the recommendation related to improving application control of unauthorized software. However, VA asserts that application controls regarding prohibited software is no longer a contributor to the information technology material weakness, or even an area of significant enterprise deficiency. VA continues to strengthen the enterprise security posture in this area as installation of software is limited to enterprise-approved applications by authorized users. These efforts significantly restrict the ability for VA users to conduct unauthorized changes or install unauthorized system software. VA's application control initiative is implemented through a deny list (blacklist) approach for prohibited software instances on endpoints. VA uses an automated endpoint client to block attempts to install all prohibited software.

OIG did not identify the installation of any prohibited software on any endpoint in any system boundaries.

In FY 2023, VA OIT made significant progress towards the resolution of these recommendations:

- 100% of prohibited applications were blocked on Windows-based end points.
- Implemented a continuous monitoring process through a system that categorizes applications within the VA environment and provides visibility.

Remediation Goals:

In support of VA's continual improvement model, in FY 2024/2025, VA will review risks and make determinations on the following use cases:

- VA OIT will review risk and available capabilities for implementation of an application control solution:
 - For the Windows server operating system: deny listing by May 15, 2024.
 - For workstation-based endpoint: protection product by May 15, 2024.
 - For the Windows client: deny listing by June 28, 2024.
 - For the server: allow listing by June 30, 2025.
 - For the Windows client: allow listing by September 30, 2025.
- VA OIT will implement, update and simplify Technical Reference Model classifications to authorized, authorized with constraints, or prohibited by October 2, 2024.

OIG FISMA Recommendation 24

NFR: 6.05

Recommendation 24: We recommended the Assistant Secretary for Information and Technology develop a comprehensive inventory process to identify connected hardware, software, and firmware used to support VA applications and operations.

Comments: Concur.

Strategic Response and Accomplishments:

VA concurs with Recommendation 24 to develop a comprehensive inventory process to identify connected hardware, software and firmware used to support VA applications and operations.

In FY 2023, VA made the following improvements to address the identified recommendation:

- Achieved 95% compliance in validation of enterprise software inventory aligned to OMB M-22-18 requirements.
- Achieved 98% compliance with enterprise hardware physical inventory requirements.
- Improved the accuracy of connected hardware and software inventory and rolled out the automated categorization of asset inventory to all sites across VA.
- Required area managers to validate assets associated with their system boundary.
- Implemented an Enterprise Software Asset Management initiative to define OIT's software asset management processes.
- Developed enterprise software inventory requirements with six-month update intervals.

Remediation Goals:

VA will complete work towards the following objectives to resolve the identified weaknesses in hardware and software inventory:

- Align 95% of hardware logical inventory with correct system boundary by September 30, 2024.
- Develop training against the monthly validation requirements of connected logical assets by July 30, 2024.
- Maintain 95% compliance with monthly reviews and validation of connected logical hardware assets within inventory system on record.
- Complete assessments of license ownership and existing software management processes across to determine the scope of software inventory by October 31, 2026.
- Develop a project plan to complete intake of designated software products into a software asset inventory by April 30, 2025.

OIG FISMA Recommendation 25

NFR: N/A

Recommendation 25: We recommended the Assistant Secretary for Information and Technology implement improved procedures for monitoring contractor-managed systems and services and ensure information security controls adequately protect VA sensitive systems and data.

Comments: Concur.

Strategic Response and Accomplishments:

VA concurs with Recommendation 25 to implement improved procedures for monitoring contractor-managed systems and services and ensure information security controls adequately protect VA sensitive systems and data.

Remediation Goals:

In FY 2024, VA will address the following enterprise-level weaknesses identified with improved procedures for monitoring contractor-managed systems:

- Update VA Handbook 6500.6 to address specific contractor-managed security measures.
- Update VA Directive 6517, Risk Management Framework for Cloud Computing Services, for alignment with Federal Risk and Authorization Management Program authorization processes.
- Integrate specific security requirements for Federal Information Technology Acquisition Reform Act review board acquisition request and approval.

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

Report Distribution

VA Distribution

Office of the Secretary
Veterans Benefits Administration
Veterans Health Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel
Office of Acquisition, Logistics, and Construction
Board of Veterans' Appeals

Non-VA Distribution

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

OIG reports are available at www.vaoig.gov.