US DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS HEALTH ADMINISTRATION

Follow-up Information Security Inspection at the VA Financial Services Center in Austin, Texas

Information Security Inspection	**23-02186-97**	**May 30, 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.

Executive Summary

Information security controls protect VA systems and data from unauthorized access, use, modification, or destruction. To determine compliance with the Federal Information Security Modernization Act of 2014 (FISMA), the VA Office of Inspector General (OIG) contracts with an independent public accounting firm to conduct an annual audit of VA's information security program and practices.[1] The FISMA audit is conducted in accordance with guidelines issued by the Office of Management and Budget and applicable National Institute of Standards and Technology (NIST) information security guidelines.[2]

The fiscal year 2022 FISMA audit reported that VA continues to face significant challenges meeting the law's requirements. The audit made 26 recommendations to VA, including repeat recommendations, to address deficiencies in configuration management, security management, and access controls.[3] Appendix A details these recommendations.

In 2020, the OIG started an information security inspection program. These inspections assess whether VA facilities are meeting federal security requirements related to control areas the OIG determined to be at highest risk.[4] Typically, facilities selected for these inspections either were not included in the annual FISMA audit sample or had previously performed poorly. The OIG conducted this follow-up inspection of the Financial Services Center (FSC) in Austin, Texas, to determine whether the FSC was meeting federal security guidance. The OIG previously inspected the FSC in 2021 and made numerous recommendations to correct identified security weaknesses.[5] During the follow-up information security inspection, the inspection team reviewed configuration management, security management, and access controls at the FSC. The team evaluated these controls because the OIG determined the areas to be at highest risk of not adequately protecting veteran-sensitive data hosted at the FSC.

This inspection identified continuing significant deficiencies related to configuration management, security management, and access controls designed to protect FSC systems from unauthorized access, alteration, or destruction. Consequently, the OIG continues to see

[1] Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. §§ 3551–3558.

[2] NIST Special Publication 800-53, rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020, includes updates as of December 10, 2020.

[3] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2022*, Report No. 22-01576-72, May 17, 2023.

[4] The 2021 inspection looked at four control areas; however, since then the OIG removed the fourth control area—contingency planning—from its information security inspection program because this area is largely enterprise controlled and is not a significant risk at the local level. Appendix B presents background information on federal information security requirements.

[5] VA OIG, *Inspection of Information Technology Security at the VA Financial Services Center*, Report No. 21-01221-24, March 31, 2022.

information security deficiencies at the FSC similar in type and risk level to the findings from the 2021 inspection and an overall inconsistent implementation and enforcement of security controls. Table 2 (pages 6 and 7) summarizes findings and recommendations from the initial FSC information security inspection and whether management has implemented effective controls to address prior recommendations. The inspection scope and methodology are described in appendix C.

The OIG's inspections are focused on three security control areas:

1. **Configuration management controls** identify and manage security features for all hardware and software components of an information system.[6]
2. **Security management controls** "establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures."[7]
3. **Access controls** provide reasonable assurance that computer resources are restricted to authorized individuals. Access also includes physical and environmental controls associated with physical security, such as authorization, visitors, monitoring, delivery, and removal.[8]

Although the findings and recommendations in this report are specific to the FSC, other VA facilities could benefit from reviewing this information and considering these recommendations.

What the Inspection Found

The OIG identified deficiencies in all three areas: configuration management, security management, and access controls.

Four Configuration Management Controls Had Deficiencies

The FSC had deficiencies in four configuration management controls:

- **Vulnerability management and flaw remediation** is the process by which the Office of Information and Technology (OIT) identifies, classifies, and reduces weaknesses. Flaw remediation is how organizations correct software defects and often includes system updates, such as security patches. This is a repeat finding from the prior site inspection.[9]

[6] Government Accountability Office (GAO), *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G, February 2009.

[7] GAO, *FISCAM*.

[8] GAO, *FISCAM*.

[9] NIST Special Publication 800-53.

- **Database scans** are used to specifically identify whether databases are compliance with VA approved secure baseline configurations. This is a new finding.
- **Database baseline configurations** are formally reviewed and agreed-upon specifications that serve as the basis for future builds, and releases or changes to systems that include security and privacy control implementation. This is a new finding.
- **Unsupported components** occur when vendors no longer update their products. This is a new finding.

Vulnerability Management and Flaw Remediation

Prior FISMA audits have repeatedly found deficiencies in VA's vulnerability management program. Consistent with those findings, the team found operating systems at the FSC that were no longer supported by the vendor and applications that were missing security patches. OIT scans for vulnerabilities routinely, randomly, and as new vulnerabilities are identified and reported. Although the inspection team and OIT used the same vulnerability-scanning tools, the OIG found 86 critical vulnerabilities that OIT did not identify during scanning processes. The inspection team also identified 497 vulnerabilities—167 critical vulnerabilities on 624 distinct devices and 330 high-risk vulnerabilities on 1,706 distinct devices—that were not mitigated within the required 30- or 60-day windows. Compared to the 2021 inspection, the FSC has over 400 percent more critical and 50 percent more high-risk vulnerabilities. Since the last inspection, the FSC made changes to divide one system boundary into two system boundaries. The boundary change resulted in the OIG identifying network segments that were not monitored and likely contributed to the higher number of vulnerabilities. While OIT is aware of many of the vulnerabilities, plans of action and milestones were incomplete.[10]

Despite the FSC's flaw remediation measures, the inspection team identified several devices missing critical security patches or using operating systems no longer supported by the vendor. For instance, the selected devices with critical and high-risk vulnerabilities had security patches available that were not applied. Without these controls, critical systems may be at unnecessary risk of unauthorized access, alteration, or destruction.

Database Scans

OIT requires database scans on a quarterly basis. However, OIT could not provide evidence of scans for all five databases supporting the FSC. Data stored within databases has become a target of attack for malicious users, with increased frequency. The effect of such an attack can result in

[10] Plans of action and milestones identify tasks necessary to address a vulnerability, deficiency, or risk and detail resources required to accomplish the tasks, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

identity theft, credit card theft, financial loss, or loss of privacy. Without periodic database scans, OIT is unaware of security control weaknesses that could adversely impact the security posture of other systems supporting the facility.

Database Baseline Configurations

The OIG identified the five local databases that had multiple vulnerabilities caused by configurations that deviated from OIT's security baseline. Without managing and applying baseline security configurations, OIT is unaware of weaknesses that could adversely impact databases and other systems.

Unsupported Components

The OIG identified 18 network switches using operating systems that did not meet OIT baseline security requirements of which six operating systems were no longer supported by the vendor. Consequently, these devices did not receive maintenance or vulnerability security updates, creating an opportunity for adversaries to exploit weaknesses in components.[11] Noncurrent software may be vulnerable to malicious code.[12] Upgrading is not just a defensive strategy but a practical one that protects network stability.

One Security Management Control Was Deficient

The OIG identified one security management control weakness involving continuous monitoring of component inventory, which is a repeat finding from the prior inspection. Specifically, the inspection team discovered almost twice the number of devices on the network when compared to those identified within the Enterprise Mission Assurance Support Service (eMASS). During the 2021 inspection, the OIG discovered more than double the devices on the network compared to those identified by the FSC. The lack of device visibility demonstrates that the FSC's continuous monitoring program still needs improvement.

The cybersecurity management service is VA's approach for workflow automation and continuous monitoring, which provides managers with information about the system and its security posture to support risk management and authorization decisions. The information security officer and system steward are responsible for identifying the facility's network ranges of device internet protocol addresses so the Cybersecurity Operations Center can perform network vulnerability scans. The inaccurate network ranges contributed to the system owner and steward not updating the inventory in eMASS to accurately reflect hardware located at the facility. By not periodically updating the hardware inventory in eMASS, managers are making risk decisions based on inaccurate system information.

[11] NIST Special Publication 800-53.

[12] GAO, *FISCAM*.

Two Access Controls Had Deficiencies

During the inspection, the team identified two deficiencies in the following access controls:

- **Audit and monitoring** involve the collection, review, and analysis of events for indications of inappropriate or unusual activity. These controls should be routinely used to assess the effectiveness of other security controls, recognize an attack, and to investigate during or after an attack. This is a repeat finding from the prior site inspection.
- **Reviewing physical access logs** can help identify suspicious activity, anomalous events, or potential threats. This is a new finding.

During the 2021 inspection, the team identified several systems that failed to generate and forward audit log data for analysis. The team validated in the current inspection that the audit logging weaknesses were corrected for those systems. However, the OIG identified a lack of audit logging on other databases and servers, indicating that the FSC's audit and monitoring program still needs improvement. OIT has a tool that performs automated audit logging and monitoring. However, OIT was unable to locate certain servers and databases in the tool to enable audit logging for those systems. Logs frequently help with incident analysis and provide information such as which accounts were accessed and what actions were performed. If this information is not available, an investigation may be limited or unsuccessful in determining whether an unauthorized use of the system or unauthorized modification of system data occurred.

Physical access logs to the data center and communication rooms were not reviewed as required by OIT policy.[13] The FSC uses a centralized system to control physical access to these areas and to maintain access logs for them. The facility manager is required to review access logs on a quarterly basis. Reviewing physical access logs can help identify suspicious activity, anomalous events, or potential threats.[14] The lack of log reviews increases the likelihood that potential threats are not identified and could result in loss of confidentiality, integrity, or access to VA sensitive data.

What the OIG Recommended

The OIG made eight recommendations to the assistant secretary for information and technology and chief information officer:

[13] Financial Technology Service, Financial Services Center, "Physical and Environmental Protection," February 21, 2023.

[14] Examples of suspicious activity are access outside of normal work hours, repeated access to areas not normally accessed, access for unusual lengths of time, or access that is out of sequence.

1. Implement a more effective vulnerability management program to address security deficiencies identified during the inspection. (This is a repeat recommendation from the prior inspection.)
2. Ensure vulnerabilities are remediated within OIT's established time frames. (This is a repeat recommendation from the prior inspection.)
3. Ensure all servers and databases are part of the automated scanning process.
4. Implement approved baseline configurations for databases and document justifications and approvals for any deviations.
5. Implement more effective configuration control processes to ensure network devices maintain vendor support and receive security updates.
6. Implement an improved inventory process to ensure the accuracy of network ranges managed within the Enterprise Mission Assurance Support Service. (This is a repeat recommendation from the prior inspection.)
7. Implement an effective audit and monitoring process for all servers and databases. (This is a repeat recommendation from the prior inspection.)
8. Ensure that physical access logs for the data center and communication rooms are reviewed on a quarterly basis.

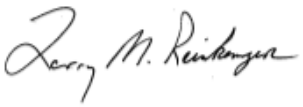
VA Management Comments and OIG Response

The assistant secretary for information and technology and chief information officer concurred with recommendations 1–4 and 6–8 and requested recommendations 1–4, 6, and 8 be closed due to corrective actions he said were completed. For recommendations 1–4 and 6–8, the planned corrective actions are responsive to the intent of the recommendations. The full text of the assistant secretary's response is included in appendix D. The assistant secretary provided sufficient evidence to support that actions taken in response to recommendations 1, 3, 4, 6, and 8 were completed, and the OIG considers these recommendations closed.

Regarding recommendation 2, while the assistant secretary requested closure of the recommendation, the evidence provided to support his request did not fully address the OIG's findings and recommendation regarding vulnerability remediation. Specifically, OIT's remediation process was developed to link identified vulnerabilities to corresponding plans of actions and milestones to mitigate security deficiencies. While the OIG recognizes this process is the first step toward correcting the deficiency, the evidence provided did not demonstrate that vulnerabilities will be remediated within established time frames. Accordingly, the OIG will continue to monitor OIT's process for remediating vulnerabilities within organizational timelines during future information security inspections.

The assistant secretary did not concur with recommendation 5 and indicated that OIT has implemented effective configuration control processes to ensure network devices maintain vendor support and receive security updates. While the assistant secretary provided evidence that six of the network devices the OIG identified were updated and supported by the vendor, OIT did not provide documentation to demonstrate the remaining 12 network devices were updated to meet baseline security requirements. Accordingly, the OIG disagrees with management's assertion that OIT has implemented effective configuration control processes and stands by its recommendation. The OIG will monitor implementation of the planned actions and will close the open recommendations when VA provides evidence demonstrating progress in addressing the issues identified.

Regarding recommendation 7, the assistant secretary stated appropriate FSC staff will develop a predetermined, recurring check within the defined systems to allow for continuous monitoring. The OIG will monitor implementation of the planned actions addressing recommendation 7 and will close it when VA provides evidence demonstrating progress in addressing the issue identified.



LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

Contents

Abbreviations

eMASS	Enterprise Mission Assurance Support Service
FISCAM	*Federal Information System Controls Audit Manual*
FISMA	Federal Information Security Modernization Act of 2014
FSC	Financial Services Center
GAO	Government Accountability Office
IT	information technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information and Technology

Introduction

Information security controls protect VA systems and data from unauthorized access, use, modification, or destruction. To determine compliance with the Federal Information Security Modernization Act of 2014 (FISMA), the VA Office of Inspector General (OIG) contracts with an independent public accounting firm that conducts an annual audit of VA's information security program and practices.[15] The FISMA audit is conducted in accordance with guidelines issued by the Office of Management and Budget and applicable National Institute of Standards and Technology (NIST) information security guidelines.[16]

In 2020, the OIG started an information security inspection program. These inspections assess whether VA facilities are meeting federal security requirements that protect systems and data from unauthorized access, use, modification, or destruction.[17] Typically, facilities selected for these inspections either were not included in the annual FISMA audit sample or had previously performed poorly. The OIG conducted this inspection to determine whether the Financial Services Center (FSC) in Austin, Texas, was meeting federal security guidance. The OIG selected the FSC as a follow-up inspection due to the financial risk associated with its operations and due to significant security weaknesses identified during the prior site inspection performed in 2021.[18] Inspections provide recommendations to VA on enhancing information security oversight at local and regional facilities.[19] Appendix C provides more detail on the inspection scope and methodology.

Although the findings and recommendations in this report are specific to the FSC, other VA facilities could benefit from reviewing this information and considering these recommendations.

[15] Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. §§ 3551–3558.

[16] NIST Special Publication 800-53, rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020, includes updates as of December 10, 2020.

[17] The 2021 inspection looked at four control areas; however, since then the OIG removed the fourth control area—contingency planning—from its information security inspection program because this area is largely enterprise controlled and is not a significant risk at the local level. Appendix B presents background information on federal information security requirements.

[18] VA OIG, *Inspection of Information Technology Security at the VA Financial Services Center*, Report No. 21-01221-24, March 31, 2022.

[19] The OIG provided VA with a memorandum related to this inspection containing "VA Sensitive Data" as defined in 38 U.S.C. § 5727. Federal law, including FISMA and its implementing regulations, requires federal agencies to protect sensitive data and information systems due to the risk of harm that could result from improper disclosure. Accordingly, the memorandum is not being published by the OIG or distributed outside of VA to prevent intentional or inadvertent disclosure of specific vulnerabilities or other information that could be exploited to interfere with VA's network operations and adversely affect the agency's ability to accomplish its mission.

Security Controls

Both the Office of Management and Budget and NIST provide criteria to evaluate security controls. These criteria provide requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system.[20]

According to VA Handbook 6500, responsibility for developing and maintaining information security policies, procedures, and control techniques lies with the assistant secretary for information and technology, who also serves as VA's chief information officer. In addition, VA Handbook 6500 describes the risk-based process for selecting system security controls, including the operational requirements.[21] VA established guidance outlining both NIST and VA-specific requirements to help information system owners select the appropriate controls to secure their systems.

OIG information security inspections are focused on three security control areas that apply to local facilities and have been selected based on their level of risk, as shown in table 1.

Table 1. Security Controls Evaluated by the OIG

Control area	Purpose	Examples evaluated
Configuration management	Identify and manage security features for all hardware and software components of an information system.	Component inventory, baseline configurations, configuration settings, change management, vulnerability management, and flaw remediation
Security management	Ensure continuous and effective risk assessment, including development, implementation, and monitoring of security procedures.	Risk management, assessment, authorization, and continuous monitoring of network device inventory
Access	Provide reasonable assurance that computer resources are restricted to authorized individuals.	Access enforcement, identification, authentication, audit, and accountability, including related physical security controls

Source: VA OIG analysis.

Without these critical controls, VA's systems are at risk of unauthorized access or modifications. A cyberattack could disrupt access to, destroy, or allow malicious control of personal

[20] Office of Management and Budget (OMB), "Security of Federal Automated Information Resources," app. 3 in OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016; NIST Special Publication 800-53.

[21] VA Handbook 6500, *Risk Management Framework for VA Information Systems: VA Information Security Program*, February 2021.

information belonging to patients, dependents, beneficiaries, VA employees, contractors, or volunteers.

Office of Information and Technology Structure and Responsibilities

The assistant secretary for information and technology and chief information officer leads the Office of Information and Technology (OIT). According to VA, OIT delivers available, adaptable, secure, and cost-effective technology services to VA. The Cybersecurity Operations Center, which is part of OIT's Office of Information Security, is responsible for protecting VA information and information systems by identifying and reporting emerging and imminent threats and vulnerabilities. OIT's Office of Development, Security, and Operations unifies software development, software operations, service management, information assurance, cybersecurity compliance, performance monitoring, and technical integration throughout the entire solution delivery process.

The Office of Information Security; Cybersecurity Operations Center; Office of Development, Security, and Operations; and End User Operations are the OIT offices relevant to the areas assessed at the FSC, as shown in figure 1.

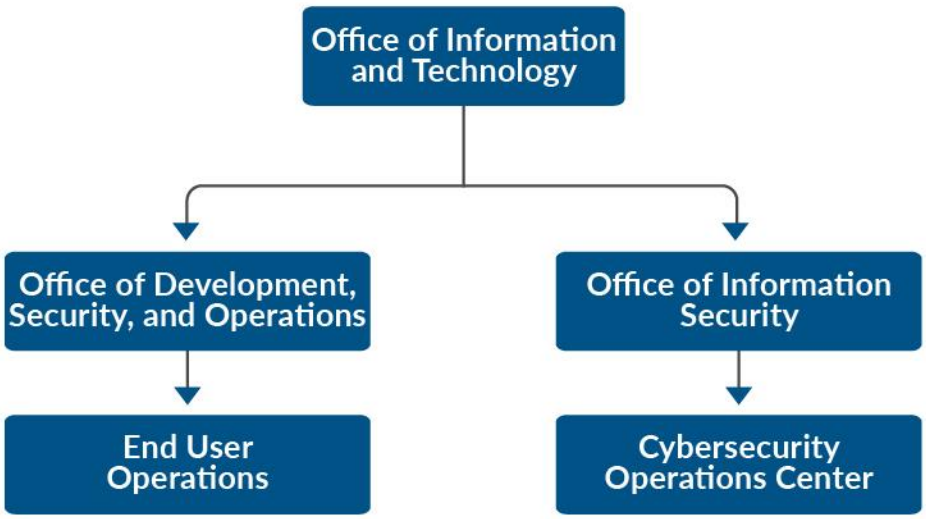


Figure 1. *Organizational structure of Office of Information and Technology entities relevant to this inspection.*
Source: VA OIG analysis.

End User Operations provides on-site and remote support to IT customers across all VA administrations and program offices, including direct support of approximately 400,000 VA employees and approximately 100,000 contractors with government-furnished IT equipment and access. End User Operations provisions computing devices, activates new facilities, executes local system implementations, and engages VA's customers across the nation to meet IT support needs. OIT assigns dedicated End User Operations and Office of Information Security personnel

to the FSC, including system stewards responsible for managing system plans of action and milestones to ensure all assessed and scanned vulnerabilities are documented.

Results of Previous Projects

As previously mentioned, the OIG issues annual reports on VA's information security program. The FISMA audit is conducted in accordance with guidelines issued by the Office of Management and Budget and applicable NIST information security guidelines.[22] The fiscal year 2022 FISMA audit, conducted by independent public accounting firm CliftonLarsonAllen LLP, evaluated 47 major applications and general support systems hosted at 23 VA facilities, including the testing of selected management, technical, and operational controls outlined by NIST.[23] CliftonLarsonAllen LLP made 26 recommendations, listed in appendix A. All 26 recommendations are repeated from the prior annual audit, indicating that VA continues to face significant challenges in complying with FISMA requirements.[24] Repeat recommendations included addressing deficiencies in configuration management, security management, and access controls.

The OIG conducted an information security inspection of the FSC in 2021. During that inspection, the OIG identified deficiencies with configuration management, security management and access controls, including specific deficiencies in component inventory, vulnerability management, flaw remediation, physical security, and audit and monitoring controls. Consequently, the team evaluated those controls during the reinspection to determine if VA has taken appropriate corrective actions.

A Government Accountability Office (GAO) statement prepared for a House Veterans' Affairs subcommittee hearing in November 2019 said VA was one of the federal agencies that continued to have a deficient information security program.[25] According to GAO, VA faced several security challenges while securing and modernizing its information systems, including:

- effectively implementing information security controls,
- mitigating known vulnerabilities,

[22] OMB Memo M-21-02, "Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements," November 9, 2020; NIST Special Publication 800-53.

[23] OMB, "Security of Federal Automated Information Resources," app. 3 in OMB Circular A-130, July 28, 2016. The circular's appendix defines a general support system as an interconnected set of information resources under the same direct management control that shares common functionality.

[24] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2022*, Report No. 22-01576-72, May 17, 2023. Appendix B presents information about FISMA and other federal criteria and standards discussed in this report.

[25] GAO, *Information Security: VA and Other Federal Agencies Need to Address Significant Challenges*, GAO-20-256T, November 14, 2019.

- establishing elements of its cybersecurity risk management program,
- identifying critical cybersecurity staffing needs, and
- managing IT supply chain risks.

GAO concluded that "until VA adequately mitigates security control deficiencies, the sensitive data maintained on its systems will remain at increased risk of unauthorized modification and disclosure, and the system will remain at risk of disruption."[26]

Financial Services Center

The FSC (shown in figure 2) is a VA fee-for-service organization that offers a wide range of financial accounting products and services to both VA and other government agencies. FSC services are organized around revenue centers and product lines to better focus service delivery and accountability. In FY 2022, the FSC processed $9.8 billion in salary and benefits for over 100,000 employees, paid more than $20.5 billion in commercial invoices, and processed $7.1 million in medical claims.

Figure 2. *Financial Services Center.*
Source: VA OIG inspection team, March 25, 2023.

[26] GAO, *Information Security: VA and Other Federal Agencies Need to Address Significant Challenges*.

Results and Recommendations

The inspection team reviewed configuration management, security management, and access controls at the FSC. The team evaluated these controls during the follow-up information security site inspection because the OIG determined the areas to be at highest risk of not adequately protecting veteran-sensitive data hosted at the FSC. The follow-up inspection continued to identify significant deficiencies related to configuration management, security management, and access controls designed to protect FSC systems from unauthorized access, alteration, or destruction. Consequently, the OIG continues to see information security deficiencies similar in type and risk level as identified in the previous audit, as well as overall inconsistent implementation and enforcement of security controls. Table 2 summarizes the findings and recommendations from the initial FSC information security inspection and whether management has implemented effective controls to address prior recommendations.

Table 2. Security Controls Evaluated During Follow-up Site Visit

Control area	Purpose	Prior site finding: FY 2021	Prior recommendations	Repeat finding: FY 2023
Configuration management	"Identify and manage" security features for all hardware and software components of an information system.[27]	OIT did not detect all vulnerabilities identified by the OIG.	Implement a more effective patch and vulnerability management program that can accurately identify vulnerabilities and enforce patch application within organizational timelines.	Yes
Security management	Establishes "a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of the procedures."[28]	The FSC did not have procedures for how to maintain systems and information integrity.	Implement system and information integrity procedures that detail how policies are applied to local systems and create a mechanism for informing employees of new or updated policies and procedures.	No

[27] GAO, *Federal Information System Controls Audit Manual (FISCAM),* GAO-09-232G, February 2009.

[28] GAO, *FISCAM*.

Control area	Purpose	Prior site finding: FY 2021	Prior recommendations	Repeat finding: FY 2023
		The FSC did not have accurate asset inventories.	Implement measures to maintain an accurate system inventory.	Yes
Access	Provide reasonable assurance that computer resources are restricted to authorized individuals. Access also includes physical and environmental controls associated with physical security like authorization, visitors, monitoring, delivery, and removal.	FSC systems failed to generate or forward audit logs for analysis.	Develop and implement capabilities for all FSC systems to generate audit logs and collect and forward audit events to the Cybersecurity Operations Center for review, analysis, and reporting.	Yes
		FSC video surveillance system was not fully functional.	Continue to upgrade the video surveillance system and ensure new capabilities provide full surveillance and video retention to improve monitoring and incident response.	No

Source: VA OIG analysis.

While the FSC has matured its configuration management processes to address some deficiencies, the OIG has repeatedly identified security weaknesses related to vulnerability management and flaw remediation designed to protect sensitive information hosted at the FSC. Additionally, the inspection team also identified deficiencies with database vulnerability scans, database baseline configurations, and unsupported infrastructure components.

During the OIG's review of security management controls, the team identified a recurring deficiency with continuous monitoring controls. Specifically, the FSC faces challenges with maintaining an accurate inventory of devices on its networks. For example, the team identified approximately 400 percent more critical-risk and 50 percent more high-risk vulnerabilities during the current inspection compared to the inspection in 2021, resulting in a repeat finding and recommendation. By not periodically updating the hardware inventory, managers are making risk decisions based on inaccurate system information. The lack of device visibility demonstrates that the FSC's continuous monitoring program still needs improvement.

Finally, the review of access controls continued to identify deficiencies in audit and monitoring controls as well as physical access. During the previous inspection, the OIG identified several systems that failed to generate and forward audit log data for analysis. The team validated that the audit logging weakness for those previously identified systems was corrected, and management has made progress implementing automated tools for managing access controls. However, the OIG identified a lack of audit logging on other databases and servers at the facility, demonstrating that the FSC's audit and monitoring controls still need improvement.

I. Configuration Management Controls

According to the GAO's *Federal Information System Controls Audit Manual* (*FISCAM*), configuration management involves identifying and managing security features for all hardware, software, and firmware components of an information system at a given point and systematically controlling changes to that configuration during the system's life cycle. Effective configuration management prevents unauthorized changes to information system resources and provides reasonable assurance that systems are configured and operating securely and as intended. The inspection team reviewed two configuration management critical elements: conduct routine configuration monitoring and update software on a timely basis.

An effective configuration management process should be described in a configuration management plan and implemented according to the plan.[29] VA should first establish an accurate component inventory to identify all devices on the network.[30] The component inventory affects the success of other controls, such as vulnerability and patch management. OIT's Cybersecurity Operations Center identifies and reports on threats and vulnerabilities. Vulnerabilities that cannot be remediated by OIT's Enterprise Vulnerability Management are assigned to system personnel for action. This process helps to secure devices from attack.

Finding 1: The Financial Services Center Had Deficiencies in Four Configuration Management Controls

To assess configuration management controls, the inspection team interviewed the information system security officer, and the system steward. The team reviewed local policies, procedures, and inventory lists and scanned the FSC's network to identify devices. The team compared the devices found on the network with the device inventories provided by VA, received vulnerability lists provided by OIT, and scanned the FSC's network to identify vulnerabilities.[31]

Comparisons of the vulnerability scans showed that OIT did not identify all critical or high-risk vulnerabilities in the network or remediate flaws, including unsupported versions of applications, missing patches, and vulnerable plug-ins. By not implementing more effective configuration management controls, VA is placing critical systems at unnecessary risk of unauthorized access, alteration, or destruction.

Vulnerability Management and Flaw Remediation

VA has a vulnerability management program, but it can be improved. This is a repeat finding from the prior inspection. Prior FISMA audits repeatedly found deficiencies in VA's

[29] GAO, *FISCAM*.

[30] GAO, *FISCAM*.

[31] See appendix C for additional information about the inspection's scope and methodology.

vulnerability management controls. Consistent with those findings, the team identified deficient controls at the FSC.[32] Vulnerability management is the process by which OIT identifies, classifies, and reduces weaknesses and is part of assessing and validating risks, as well as monitoring the effectiveness of a security program. The Cybersecurity Operations Center identifies and reports on threats and vulnerabilities, and OIT conducts scans for vulnerabilities both routinely and randomly, or when new vulnerabilities are identified and reported.

VA conducts periodic independent scans of all its systems. Discovered vulnerabilities are entered into a plan of action and milestones for remediation by the system steward. System stewards then use the Remediation Effort Entry Form to document the plan of action and milestones for each deficiency identified from the scan and provide evidence that the deficiencies have been mitigated.[33]

NIST assigns severity levels to vulnerabilities by using the Common Vulnerability Scoring System, a framework for communicating the characteristics of software vulnerabilities.[34] The scoring system captures the principal characteristics of a vulnerability and produces a numerical score reflecting its severity. Numerical scores are classified as severity levels (low, medium, high, or critical) to help organizations properly assess and prioritize vulnerability management processes. For example, on a scale of zero to 10, critical-severity vulnerabilities have a score between 9.0 and 10, while high-severity vulnerabilities have a score between 7.0 and 8.9. VA requires critical-severity vulnerabilities be remediated within 30 days and high-severity vulnerabilities be remediated in 60 days.[35]

The inspection team compared OIT provided network vulnerability scan results from the FSC against its own scans conducted May 22–26, 2023. The team and OIT used the same vulnerability scanning tools. The team identified 497 vulnerabilities (167 critical-risk vulnerabilities on 624 distinct devices and 330 high-risk vulnerabilities on 1,706 distinct devices) that were not mitigated within the time frames established by OIT. Moreover, OIT's security scans did not identify 86 critical-risk vulnerabilities the team detected.[36] Similarly, the prior

---

[32] GAO, *FISCAM*. Vulnerabilities are "weaknesses in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source."

[33] A system steward is an agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

[34] "Vulnerability Metrics," NIST National Vulnerability Database, accessed August 7, 2023, https://nvd.nist.gov/vuln-metrics/cvss; "Common Vulnerability Scoring System ver. 3.14, Specification Document, Revision 1," Forum of Incident Response and Security Teams, accessed August 7, 2023, https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf.

[35] Department of Veterans Affairs Information Security Knowledge Service, "Security Controls Explorer," accessed August 7, 2023 (not accessible by the public). The Information Security Knowledge Service is the approved source for VA cybersecurity and privacy policies, procedures, processes, and guidance.

[36] The difference in scan results can be attributed to multiple factors. First, the scans are conducted at different points in time, so devices could have been added to or removed from the network between scans. Finally, the scans are conducted from different places in the network, which could be impacted by access controls.

FISMA audit found that "VA did not have a complete inventory of all vulnerabilities present on locally hosted systems."[37] The OIG identified critical and high-risk vulnerabilities on 27 percent of the devices at the FSC.

During the 2021 information security inspection, the team identified 252 vulnerabilities (32 critical-risk vulnerabilities on 122 devices and 220 high-risk vulnerabilities on 222 devices) that were not mitigated within the time frames established by OIT. Therefore, the OIG's recent inspection identified over 400 percent more critical-risk and 50 percent more high-risk vulnerabilities. The FSC made changes to their system boundaries by dividing one system boundary into two system boundaries and the OIG identified network segments that were not being monitored, which likely contributed to the higher number of vulnerabilities.[38]

While OIT is aware of many of the vulnerabilities, its vulnerability management process was not always followed. Specifically, its plans of action and milestones did not list specific vulnerabilities, strategies for remediation, or any resource constraints.[39] The system steward was able to demonstrate OIT's updated process for tracking vulnerabilities to plans of action and milestones since the team's first inspection. However, the data were incomplete. Without an effective vulnerability management program, vulnerabilities such as security and functionality problems in software and firmware might not be mitigated, increasing opportunities for exploitation.

VA uses its Information Central Analytics and Metrics Platform to communicate security vulnerabilities to facilities for remediation. The OIG found that the information within the platform was not complete and accurate. For example, the May 2023 reports contained 1,543 entries for critical-, high-, and medium-risk host vulnerabilities. However, the inspection team found that OIT's scans for the same period contains 51,443 entries for critical-, high-, and medium-risk vulnerabilities. Not having complete and accurate information in the vulnerability reports can undermine managers' abilities to take appropriate corrective actions.

During the 2021 inspection, the team identified 32 critical-risk vulnerabilities that were not mitigated within time frames established by OIT. In the recent inspection, the team identified five critical-risk vulnerabilities in its scans conducted May 22–26, 2023, that were previously identified in the 2021 inspection. The vulnerabilities, which are related to unsupported software and missing security patches, did not exist on the same devices as the previous inspections.

---

[37] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2022*.

[38] This is discussed further under the section "Lack of Continuous Monitoring for Inventory" in finding 2.

[39] Plans of action and milestones identify tasks that need to be accomplished. They detail resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. They also describe the measures planned to correct deficiencies identified in the controls and to address known vulnerabilities. For information security inspections, the OIG considers a vulnerability managed—even if it still exists—if the plan of action and milestones accurately identifies the devices impacted and details mitigation efforts, and the schedule of milestones is accurate and timely.

However, the OIG's identification of unmitigated vulnerabilities two years later indicates that the FSC's flaw remediation program still needs improvement.

The FSC did not remediate all flaws affecting devices in its network, which is a repeat finding from the prior inspection. For example, the inspection team identified vulnerabilities, such as operating systems that were no longer supported by the vendor and applications with missing security patches. The flaw remediation process identifies, reports, and corrects system flaws, including installing security-relevant software and firmware updates.[40] Security-relevant updates include patches, service packs, and malicious code signatures. Security patches are usually the most effective way to mitigate software flaw vulnerabilities. According to GAO, a patch is a piece of software code inserted into a program to temporarily fix a defect. NIST further explains that patches correct security and functionality problems in software and firmware. Patch management is how OIT acquires, tests, applies, and monitors updates that address security and functionality problems. Patch management is a critical process used to help alleviate many of the challenges in securing systems from cyberattack. Previous FISMA audits have repeatedly found deficiencies in this area.[41]

Database Scans Not Performed

Database scans are used to specifically identify whether databases are compliance with VA approved secure baseline configurations. OIT requires database scans to be performed on a quarterly basis. However, the FSC could not provide evidence of scans for all five databases supporting it. The FSC could not provide a reason for the limited scans. Data stored within a database management system have become a target of attack for malicious users with increased frequency. The effect of such an attack can result in identity theft, financial loss, or loss of privacy. Without periodic database scans, the FSC is unaware of security control weaknesses that could adversely impact the security posture of databases and other systems supporting the facility.

Database Did Not Meet Baseline Configurations

The OIG identified five local databases with multiple vulnerabilities caused by configurations that deviated from the OIT security baseline.[42] The baseline is a guide that provides policy, guidance, and implementation of secure baseline configurations for the databases. Further, four

[40] NIST Special Publication 800-53.

[41] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2022*; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2021*, Report No. 21-01309-74, April 13, 2022; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2020*, Report No. 20-01927-104, April 29, 2021.

[42] Database baseline configurations are formally reviewed and agreed-upon specifications that serve as the basis for future builds, and releases or changes to systems that include security and privacy control implementation.

of the databases did not have the latest security update installed, which would address many vulnerabilities identified in the vulnerability management and flaw remediation testing. Without managing and applying baseline configuration, OIT is unaware of weaknesses that could adversely impact the database and other systems at the FSC.

Unsupported Infrastructure Components

The OIG identified 18 network switches that used operating systems that did not meet OIT baseline requirements, of which six were no longer supported by the vendor. Consequently, these devices did not receive maintenance or vulnerability support. Unsupported system components can result in an opportunity for adversaries to exploit weaknesses in components.[43] Additionally, noncurrent software may be vulnerable to malicious code.[44] Upgrading is a defensive strategy as well as a practical one that protects network stability.

Finding 1 Conclusion

The FSC's vulnerability management controls did not identify all network weaknesses, such as unsupported versions of applications, and flaw remediation controls did not ensure comprehensive patch management. Vulnerabilities were not always remediated within time frames established by OIT. Database scans were not conducted on five databases supporting the FSC. Those same databases also deviated from approved baseline configurations. Additionally, 18 network devices were using operating systems that did not meet baselines, including six network devices that were no longer supported by the vendor. Without effective configuration management controls, managers do not have adequate assurance that the system and network will perform as intended and to the extent needed to support VA's mission.

Recommendations 1–5

The OIG made the following recommendations to the assistant secretary for information and technology and chief information officer:

1. Implement a more effective vulnerability management program to address security deficiencies identified during the inspection. (This is a repeat recommendation from the prior site inspection.)
2. Ensure vulnerabilities are remediated within the Office of Information and Technology's established time frames. (This is a repeat recommendation from the prior site inspection.)
3. Ensure all servers and databases are part of the automated scanning process.

[43] NIST Special Publication 800-53.

[44] GAO, *FISCAM*.

4. Implement approved baseline configurations for databases and document justifications and approvals for any deviations.
5. Implement more effective configuration control processes to ensure network devices maintain vendor support and receive security updates.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 1–4 and requested closure of these recommendations based on corrective actions he said were completed. In response to recommendations 1 and 2, the assistant secretary stated VA has implemented processes to ensure that future vulnerabilities will be remediated within established timeframes. For recommendations 3 and 4, the assistant secretary asserted that database security will be evaluated through an automated scanning process and baseline configuration standards have been implemented for all databases. The assistant secretary did not concur with recommendation 5, indicating OIT has implemented effective configuration control processes to ensure network devices maintain vendor support and receive security updates. The full text of the assistant secretary's response is included in appendix D.

OIG Response

The assistant secretary for information and technology and chief information officer submitted responsive action plans for recommendations 1–4. The assistant secretary provided sufficient evidence to support those actions taken in response to recommendations 1, 3, and 4 were completed, and the OIG considers these recommendations closed. Regarding recommendation 2, the evidence the assistant secretary provided in support of his request to close the recommendation did not fully address the OIG's findings and recommendation regarding vulnerability remediation. Specifically, OIT's remediation process was developed to link identified vulnerabilities to corresponding plans of actions and milestones to mitigate security deficiencies. While the OIG recognizes this process is the first step toward correcting the deficiency, the evidence provided did not demonstrate that vulnerabilities will be remediated within established time frames. Accordingly, the OIG will continue to monitor OIT's process for remediating vulnerabilities within organizational timelines during future information security inspections.

For recommendation 5, the assistant secretary provided evidence that six of the network devices the OIG identified were updated and supported by the vendor. However, OIT did not provide documentation to demonstrate the remaining 12 network devices were updated to meet baseline security requirements. Accordingly, the OIG disagrees with management's assertion that OIT has implemented effective configuration control processes and stands by its recommendation. The OIG will monitor implementation of the planned actions and will close the open

recommendations when VA provides evidence demonstrating progress in addressing the issues identified.

II. Security Management Controls

According to *FISCAM*, security management controls establish a framework and continuous cycle for assessing risk, developing security procedures, and monitoring the effectiveness of the procedures. The inspection team evaluated five security management critical elements: establish a security management program, assess and validate risk, document and implement security control policies and procedures, monitor the effectiveness of the security program, and effectively remediate information security weaknesses.[45]

Finding 2: The Financial Services Center Had One Security Management Control Deficiency

To assess security controls, the inspection team reviewed local security management policies, standard operating procedures, and applicable VA policies. Among the topics reviewed were the system security plan, security authorization and risk assessment, security control policies and procedures, and plans of action and milestones for known deficiencies. The team also interviewed the system steward, information system security officer, and facility manager. Finally, the team conducted a walk-through of the facility.

The OIG found that the FSC has a system security plan and risk assessment documented and approved by managers, and documented that security control policies and procedures are in place and are signed and approved. The FSC has developed and implemented plans of action and milestones for self-identified weaknesses. The plans of action and milestones have been periodically reviewed. However, the OIG did find a deficiency in continuous monitoring of the inventory at the FSC, which is a modified repeat finding and recommendation from the previous inspection.

Lack of Continuous Monitoring for Inventory

The OIG discovered almost twice the number of devices on the network than those identified in the Enterprise Mission Assurance Support Service (eMASS), VA's cybersecurity management service for workflow automation and continuous monitoring that provides managers with risk management information about a system and its security posture. Continuous monitoring facilitates ongoing awareness of the FSC system security and privacy posture to support organizational risk management decisions. Frequent updates to hardware and software inventories are a key component of VA's continuous monitoring program. Additionally, the information security officer and system steward are responsible for identifying the facility's network ranges of device internet protocol addresses so the Cybersecurity Operations Center can perform network vulnerability scans. The inaccurate network ranges contributed to the system

[45] *FISCAM* critical elements for security management are listed in appendix B.

owner and the system steward not updating the inventory in eMASS to accurately reflect hardware located at the facility. By not periodically updating the hardware inventory in eMASS, managers are making risk decisions based on inaccurate system information.

This finding is similar to the component inventory finding identified in the 2021 inspection. During that inspection, the OIG also discovered more than double the devices on the network compared to those identified by the FSC. The lack of device visibility indicates that the FSC's continuous monitoring program still needs improvement.

Finding 2 Conclusion

The FSC's network range was not accurately identified. Consequently, monitoring controls did not identify all components in the FSC on a continuous and timely basis. Without effective monitoring, VA cannot determine if security controls are designed appropriately and operating effectively, which could lead to managers making risk decisions based on inaccurate information.

Recommendation 6

The OIG made the following recommendation to the assistant secretary for information and technology and chief information officer:

6. Implement an improved inventory process to ensure the accuracy of the network ranges managed within Enterprise Mission Assurance Support Service. (This is a repeat recommendation from the prior inspection.)

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendation 6 and stated OIT has taken actions to electronically align assets to system boundaries. The assistant secretary requested the recommendation be closed due to corrective actions he said were completed.

OIG Response

For recommendation 6, the planned corrective actions are responsive to the intent of the recommendation. The assistant secretary provided sufficient evidence to support that actions taken in response to the recommendation were completed, and the OIG considers this recommendation closed. The full text of the assistant secretary's response is included in appendix D.

III. Access Controls

Previous FISMA reports have repeatedly identified access controls as a nationwide issue for VA. Access controls can be both logical and physical and provide reasonable assurance that computer resources are restricted to authorized individuals. Logical access controls require users to authenticate themselves, limit the resources users can access, and restrict actions they can take. Physical access controls involve restricting physical access to computer resources and protecting them from loss or impairment. At the FSC, the inspection team reviewed three critical access control elements, each of which contain multiple controls.[46]

Finding 3: The Financial Services Center Had Deficiencies in Two Access Controls

To evaluate the FSC's access controls, the inspection team interviewed the information system security officer, database administrators, and local IT specialists; reviewed local policies and procedures; and conducted walk-throughs of the facility.[47] The OIG found that the FSC did not collect and monitor audit logs for servers and databases, which is a repeat finding from the previous inspection, and physical access logs were not reviewed.

Audit and Monitoring

The OIG determined that improvements are needed for servers and databases audit logging at the FSC. Audit and monitoring controls involve the collection, review, and analysis of events for indications of inappropriate or unusual activity. These controls should be routinely used to assess the effectiveness of other security controls, to recognize an attack, and to investigate during or after an attack.[48] OIT has implemented tools that perform automated audit logging and monitoring. However, OIT was unable to locate certain servers and databases in the system monitoring tool, resulting in those systems not generating and reporting audit logs. Logs help with incident analysis and provide information such as which accounts were accessed and what actions were performed. If this information is not available, an investigation may be limited or unsuccessful in determining whether an unauthorized use of the system or unauthorized modification of system data occurred.

During the 2021 inspection, the team identified several systems that failed to generate and forward log data for analysis. The team validated during the current inspection that the audit logging weaknesses were corrected for those systems. However, the OIG identified a lack of

[46] *FISCAM*-critical elements for access controls are listed in Appendix B.

[47] See appendix C for additional information about the inspection's scope and methodology.

[48] GAO, *FISCAM*.

audit logging on other databases and servers, which demonstrates that the FSC's audit and monitoring program still needs improvement.

Monitoring Physical Access

The OIG discovered that the physical access logs were not being reviewed as required by OIT policy.[49] The FSC uses a centralized system to control physical access to the data center and communication rooms, and the system maintains access logs to those rooms. The facility manager is required to review access logs on a quarterly basis. Reviewing physical access logs can help identify suspicious activity, anomalous events, or potential threats.[50] This is a new finding. The lack of log reviews increases the likelihood that potential threats are not identified, which could result in the loss of confidentiality or integrity of VA sensitive data or loss of access to those data.

Finding 3 Conclusion

The FSC did not implement audit and monitoring for all servers and databases—an issue that was also noted in the 2021 inspection—and physical access logs were not being reviewed in accordance with OIT policy. Unless the FSC takes corrective actions, it risks unauthorized access to critical network resources, inability to respond effectively to incidents, and loss of personally identifiable information.

Recommendations 7–8

The OIG made the following recommendations to the assistant secretary for information and technology and chief information officer:

7. Implement an effective audit and monitoring process for all servers and databases. (This is a repeat recommendation from the prior inspection.)
8. Ensure that physical access logs for the data center and communication rooms are reviewed quarterly.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 7 and 8. Regarding recommendation 7, he stated appropriate FSC staff will develop a predetermined, recurring check within the defined systems to allow for continuous monitoring. In response to recommendation 8, he stated that the FSC information log form now

[49] Financial Technology Service, Financial Services Center, "Physical and Environmental Protection," February 21, 2023.

[50] Examples of suspicious activity are access outside of normal work hours, repeated access to areas not normally accessed, access for unusual lengths of time, or access that is out of sequence.

includes a field for information security officers to sign after reviewing the logs. The assistant secretary requested closure of recommendation 8 due to corrective actions he said were completed. The full text of the assistant secretary's response is included in appendix D.

OIG Response

For recommendations 7 and 8, the planned corrective actions are responsive to the intent of the recommendations. The assistant secretary provided sufficient evidence to support actions taken to address recommendation 8 were completed, and the OIG considers this recommendation closed. The OIG will monitor implementation of the planned actions addressing recommendation 7 and will close it when VA provides evidence demonstrating progress in addressing the issue identified. The full text of the assistant secretary's response is included in appendix D.

Appendix A: FISMA Audit for Fiscal Year 2022 Report Recommendations

In the Federal Information Security Modernization Act of 2014 (FISMA) audit for fiscal year 2022, CliftonLarsonAllen LLP made 26 recommendations. Of these, all 26 were repeat recommendations from the prior year. The FISMA audit assesses the agencywide security management program, and recommendations in the FISMA report are not specific to the Financial Services Center. The 26 recommendations are listed below.[51]

1. 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.
2. 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.
3. Implement controls to ensure that system stewards and responsible officials obtain appropriate documentation prior to closing Plans of Action and Milestones.
4. 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.
5. Implement improved processes for reviewing and updating key security documentation including control assessments on risk-based rotation as needed. Such updates will ensure all required information is included and accurately reflects the current environment.
6. Implement improved processes to ensure compliance with VA password policy and security standards on domain controls, operating systems, databases, applications, and network devices.
7. Implement periodic reviews to minimize access by system users with incompatible roles, permissions in excess of required functional responsibilities, and unauthorized accounts.
8. Enable system audit logs on all critical systems and platforms and conduct centralized reviews of security violations across the enterprise.

[51] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2022*, Report No. 22-01576-72, May 17, 2023.

9. Implement improved processes for establishing and maintaining accurate data within VA systems used for background investigations.
10. Strengthen processes to ensure appropriate levels of background investigations are completed for applicable VA employees and contractors.
11. Implement more effective automated mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and web application servers.
12. Implement a more effective patch and vulnerability management program to address security deficiencies identified during our assessments of VA's web applications, database platforms, network infrastructure, and workstations.
13. 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.
14. Implement improved network access controls that restrict medical devices from systems hosted on the general network.
15. 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.
16. Implement improved processes to ensure that all devices and platforms are evaluated using credentialed vulnerability assessments.
17. Implement improved procedures to enforce standardized system development and change control processes that integrates information security throughout the life cycle of each system.
18. Review system boundaries, recovery priorities, system components, and system interdependencies and implement appropriate mechanisms to ensure that established system recovery objectives can be measured and met.
19. Ensure that contingency plans for all systems are updated to include critical inventory components and are tested in accordance with VA requirements.
20. Implement more effective agencywide incident response procedures to ensure timely notification, reporting, updating, and resolution of computer security incidents in accordance with VA standards.
21. Ensure that systems and applications are adequately and monitored to facilitate agencywide awareness of information security events.
22. Implement improved safeguards to identify and prevent unauthorized vulnerability scans on VA networks.

23. 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 Plans of Action and Milestones.
24. Implement improved processes to monitor for unauthorized changes to system components and the installation of prohibited software on all agency devices and platforms.
25. Develop a comprehensive inventory process to identify connected hardware, software, and firmware used to support VA programs and operations.
26. Implement improved procedures for monitoring contractor-managed systems and services and ensure information security controls adequately protect VA sensitive systems and data.

Appendix B: Background

Federal Information System Controls Audit Manual

The Government Accountability Office (GAO) developed the *Federal Information System Controls Audit Manual (FISCAM)* to provide auditors and information system control specialists a specific methodology for evaluating the confidentiality, integrity, and availability of information systems. *FISCAM* groups related controls into categories that have similar risks. To assist auditors in evaluating information systems, *FISCAM* maps control categories to National Institute of Standards and Technology (NIST) controls.

FISCAM breaks configuration management controls into the following critical elements.

- **Develop and document configuration management policies, plans, and procedures** at the entity, system, and application levels to ensure effective configuration management processes. These procedures should cover employee roles and responsibilities, change control, system documentation requirements, establishment of decision-making structure, and configuration management training.
- **Maintain current configuration information,** which involves naming and describing physical and functional characteristics of a controlled item, as well as performing activities to define, track, store, manage, and retrieve configuration items. Examples of these controls are baseline configurations, configuration settings, and component inventories.
- **Authorize, test, approve, and track changes** by formally establishing a change management process, with management's authorization and approval of the changes. This element includes documenting and approving test plans, comprehensive and appropriate testing of changes, and creating an audit trail to clearly document and track changes.
- **Conduct routine configuration monitoring** to determine the accuracy of the changes that should address baseline and operational configuration of hardware, software, and firmware.[52] Products should comply with applicable standards and the vendors' good security practices. The organization should have the ability to monitor and test to determine if a system is functioning as intended, as well as to determine if networks are appropriately configured and paths are protected between information systems.
- **Update software on a timely basis** by scanning software and updating it frequently to guard against known vulnerabilities. In addition, security software should be kept current by establishing effective programs for patch management, virus protection, and

[52] Firmware are computer programs and data stored in hardware, typically in read-only memory, that cannot be written or modified during the execution of the program.

identification of other emerging threats. Software releases should be controlled to prevent the use of noncurrent software. Examples of these controls are software usage restrictions, user-installed software, malicious code protection, security alerts, and advisories. Examples of controls in this element are vulnerability scanning, flaw remediation, malicious code protection, security alerts, and advisories.

- **Document and have emergency changes approved** by appropriate entity officials and notify appropriate personnel for follow-up and analysis of the changes. It is not uncommon for program changes to be needed on an emergency basis to keep a system operating. However, due to the increased risk of errors, emergency changes should be kept to a minimum.

FISCAM has seven critical elements for security management:

- **Institute a security management program** that establishes policies, plans, and procedures clearly describing all major systems and facilities and that outlines the duties of those responsible for overseeing security as well as those who own, use, or rely on the organization's computer resources. There should be a clear security management structure for systems and devices as well as for business processes. Examples of specific controls are system security plans, plan updates, activity planning, and resource allocation.
- **Assess and validate risk** by comprehensively identifying and considering all threats and vulnerabilities. This step ensures that agencies address the greatest risks and appropriately decide to accept or mitigate risks. Examples of these controls are security certification, accreditation, categorization, and risk assessment.
- **Document and implement security control policies and procedures** that appropriately address general and application controls and ensure users can be held accountable for their actions. These controls, which are more general at the entity-wide level and more specific at the system level, should be approved by managers.
- **Implement security awareness and personnel policies** that provide training for new employees, contractors, and users; periodic refresher training; and distribution of security policies detailing rules and expected behaviors. This element also addresses hiring, transfers, terminations, and performance for employees, contractors, and users. Examples of controls in this area are security awareness training, rules of behavior, position categorization, personnel policies, personnel screening, termination, transfer, access agreements, third-party personnel security, and personnel sanctions.
- **Monitor the program** to ensure that policies and controls effectively reduce risk on an ongoing basis. Effective monitoring involves testing controls to evaluate and determine whether they are appropriately designed and operating effectively. Examples of these

controls are security assessments, continuous monitoring, privacy impact assessments, and vulnerability scanning.

- **Remediate information security weaknesses** when they are identified, which involves reassessment of related risks, applying appropriate corrective actions, and follow-up monitoring to ensure actions are effective. Agencies develop plans of actions and milestones to track weaknesses and corresponding corrective actions.
- **Ensure third parties are secure,** as vendors, business partners, and contractors are often granted access to systems for purposes such as outsourced software development or system transactions.[53]

FISCAM lists six access control critical elements:

- **Boundary protection controls** protect a logical or physical boundary around a set of information resources and implement measures to prevent unauthorized information exchange across the boundary. Firewall devices are the most common boundary protection technology.
- **Sensitive system resources controls** are designed to ensure the confidentiality, integrity, and availability of system data such as passwords and keys during transmission and storage. Technologies used to control sensitive data include encryption and certificate management.
- **Physical security** restricts access to computer resources and protects them from loss or impairment. Physical security controls include guards, gates, locks, and environmental controls such as smoke detectors, fire alarms and extinguishers, and uninterruptible power supplies.
- **Audit and monitoring controls** involve the collection, review, and analysis of events for indications of inappropriate or unusual activity. These controls should be routinely used to assess the effectiveness of other security controls, to recognize an attack, and to investigate during or after an attack.
- **Identification and authentication controls** distinguish one user from another and establish the validity of a user's claimed identity.
- **Authorization controls** determine what users can do, such as granting access to various resources, and depend on valid identification and authentication controls. These controls establish the validity of a user's claimed identity.

[53] GAO, *FISCAM*.

Federal Information Security Modernization Act of 2014

The following are the stated goals of FISMA:

- Provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.
- Recognize the highly networked nature of the current federal computing environment and provide effective government-wide management and oversight of the related information security risks.
- Provide for development and maintenance of minimum controls required to protect federal information and information systems.
- Provide a mechanism for improved oversight of federal agency information security programs.
- Acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions.
- Recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.[54]

FISMA also requires an annual independent assessment of each agency's information security program to determine its effectiveness. Inspectors general or independent external auditors must conduct annual evaluations. The VA Office of Inspector General (OIG) accomplishes the annual FISMA evaluation through a contracted external auditor and provides oversight of the contractor's performance.

NIST Information Security Guidelines

The Joint Task Force Interagency Working Group created the NIST information security guidelines.

[54] FISMA § 3551.

Appendix C: Scope and Methodology

Scope

The inspection team conducted its work from April 2023 through October 2023. The team evaluated configuration management, security management, and access controls of operational VA information security assets and resources in accordance with FISMA, NIST security guidelines, and VA's information security policy. In addition, the team assessed the capabilities and effectiveness of information security controls used to protect VA systems and data from unauthorized access, use, modification, or destruction.

Methodology

To accomplish the objective, the inspection team examined relevant laws and policies. The team also inspected the facility and systems for security compliance. Additionally, the team interviewed VA personnel responsible for the Financial Services Center's (FSC) information security and operations, privacy compliance, and facility management. The team conducted vulnerability and configuration testing to determine local systems' security compliance. Finally, the team analyzed the results of testing, interviews, and the inspection to identify policy violations and threats to security.

Internal Controls

The inspection team determined that internal controls were significant to the inspection objectives. The overall scope of information security inspections is the evaluation of general security and application controls that support VA's programs and operations. According to the risk management framework for VA information systems, the information security program is the foundation for VA's information security and privacy program and practices. The framework is documented in VA Handbook 6500.

The team used the GAO's *FISCAM* as a template to plan for inspections. When planning for this inspection, the team identified potential information system controls that would significantly impact the inspection. Specifically, the team used *FISCAM* appendix II as a guide to help develop evidence requests and a base set of interview questions for the FSC and its personnel. The team used the *FISCAM* controls identified in appendix B as an overlay to correlate FISMA controls used by VA to protect and secure its information systems. Although similar to the contractor-conducted annual FISMA audits, this inspection focused on security controls that are implemented at the local level. However, some controls overlap and are assessed in both assessments due to redundant roles and responsibilities among VA's local, regional, and national facilities and offices.

The inspection team determined that all controls applicable to the FSC aligned with the control activities category. Control activities are the actions managers establish through policies and procedures to achieve objectives and respond to risks in the internal control system, which includes the entity's information systems. When the team identified control activity deficiencies, team members assessed whether other relevant controls contributed to those deficiencies. The team did not address risk assessment controls because VA's risk management framework is based on NIST security and privacy controls.

Fraud Assessment

The inspection team assessed the risk that fraud and noncompliance with provisions of laws, regulations, contracts, and grant agreements, significant within the context of the audit objectives, could occur during this inspection. The team exercised due diligence in staying alert to any fraud indicators. The OIG did not identify any instances of fraud or potential fraud during this audit.

Data Reliability

The inspection team generated computer-processed data by using network scanning tools. The results of the scans were provided to the Office of Information and Technology's (OIT) Quality and Compliance Readiness Office. The team used industry-standard information system security tools to identify information systems on the VA network and to take snapshots of their configurations, which were used to identify vulnerabilities. In this process, the team was not testing VA data or systems for transactional accuracy. The security tools identified a version of software present on a system and then compared it to the expected version. If the system did not have the current software version, the tool identified that as a vulnerability. As the security tools did not alter data, the team determined that the output was reliable. The data were complete and accurate, met intended purposes, and were not subject to alteration.

Government Standards

The OIG conducted this inspection in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation.*

Appendix D: VA Management Comments

Department of Veterans Affairs Memorandum

Date: [This line empty in original]

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

Subj: Follow-up Information Security Inspection at the VA Financial Services Center in Austin, Texas, Project Number 2023-02186-AE-0081 (VIEWS 11347602)

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

1. Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft report, Follow-up Information Security Inspection at the VA Financial Services Center in Austin, Texas (Project Number 2023-02186-AE-0081).

2. The Office of Information and Technology (OIT) submits the attached written comments, along with a target completion date or closure evidence for each of the OIG's recommendations.

The OIG removed point of contact information prior to publication.

(Original signed by)

Kurt D. DelBene

Attachment

Attachment

Office of Information and Technology

Comments on Office of Inspector General Draft Report,

Follow-up Information Security Inspection at the VA Financial Services Center in Austin, Texas, Project Number 2023-02186-AE-0081

(VIEWS 11347602)

Recommendation 1: Implement a more effective vulnerability management program to address security deficiencies identified during the inspection. (This is a repeat recommendation from the prior inspection.)

Comments: Concur.

The Department of Veterans Affairs (VA) Office of Information and Technology (OIT) has remediated all vulnerabilities and implemented a process to ensure that all future vulnerabilities will be remediated within OIT's established timeframes.

Expected Completion Date: Completed.

VA OIT requests closure of Recommendation 1.

Recommendation 2: Ensure vulnerabilities are remediated within the Office of Information and Technology's established time frames. (This is a repeat recommendation from the prior site inspection.)

Comments: Concur.

VA OIT has remediated all vulnerabilities and implemented a process to ensure that all future vulnerabilities will be remediated within OIT's established timeframes.

Expected Completion Date: Completed.

VA OIT requests closure of Recommendation 2.

Recommendation 3: Ensure all servers and databases are part of the automated scanning process.

Comments: Concur.

Several VA OIT databases have been decommissioned and they are all part of the automated scanning process outlined in VA policy.

Expected Completion Date: Completed.

VA OIT requests closure of Recommendation 3.

Recommendation 4: Implement approved baseline configurations for databases and document justifications and approvals for any deviations.

Comments: Concur.

VA OIT has implemented approved baseline configurations for all databases and documented justifications and approvals for any deviations.

Expected Completion Date: Completed.

VA OIT requests closure of Recommendation 4.

Recommendation 5: Implement more effective configuration control processes to ensure network devices maintain vendor support and receive security updates.

Comments: Non-Concur.

VA OIT has implemented effective configuration control processes to ensure network devices maintain vendor support and receive security updates.

VA OIT requests closure or removal of Recommendation 5.

Recommendation 6: Implement an improved inventory process to ensure the accuracy of network ranges managed within the Enterprise Mission Assurance Support Service. (This is a repeat recommendation from the prior inspection.)

Comments: Concur.

VA OIT has transitioned to the Enterprise Federal Information Security Modernization Act (FISMA) Containerization Asset to Boundary (FCAB) project, which electronically aligns assets to their new FISMA system boundaries. The FCAB project allows for easier identification of system owners of device assets, better vulnerability management and future baseline configuration capabilities.

For consistency of process and accuracy of data, logical hardware reporting related to inventory will be provisioned using FCAB. The new reporting shows a complete and accurate picture of logical inventory at the time of scanning.

Expected Completion Date: Completed.

VA OIT requests closure of Recommendation 6.

Recommendation 7: Implement an effective audit and monitoring process for all servers and databases. (This is a repeat recommendation from the prior inspection.)

Comments: Concur.

VA Financial Service Center (FSC) administrators, system stewards and necessary members will develop a pre-determined, recurring check of systems within the defined monitoring systems. This will allow continuous monitoring of systems and ensure they are accounted for and remain monitored.

Expected Completion Date: September 30, 2024.

Recommendation 8: Ensure that physical access logs for the data center and communication rooms are reviewed on a quarterly basis.

Comments: Concur.

VA FSC Information System Security Officers updated the log form to include their signatures after reviewing logs. The action was completed July 30, 2023.

Expected Completion Date: Completed.

VA OIT requests closure of Recommendation 8.

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

OIG Contact and Staff Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Inspection Team	Michael Bowman, Director Ginalynn Alvarado Jack Henserling Timothy Moorehead Kimberly Moss Adam Sowells Brandon Zahn
Other Contributors	Bill Warhop Clifford Stoddard

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
Director, Financial Services Center

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