DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

OFFICE OF MANAGEMENT

Inspection of Information Technology Security at the VA Financial Services Center

INFORMATION TECHNOLOGY INSPECTION | REPORT #21-01221-24 | MARCH 31, 2022

MISSION

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

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

Report suspected wrongdoing in VA programs and operations to the VA OIG Hotline:

www.va.gov/oig/hotline

1-800-488-8244

Executive Summary

Information technology (IT) 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.[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 2020 FISMA audit made 26 recommendations to VA. Repeat recommendations included addressing deficiencies across four security control areas: configuration management, contingency planning, security management, and access.[3] Appendix A details these recommendations. The report concluded that VA continues to face significant challenges meeting FISMA requirements.

In 2020, the OIG started an IT security inspection program to help identify whether VA facilities are meeting federal security requirements related to the four security control areas.[4] These IT inspections are typically conducted at selected facilities that have not been assessed under the annual audit required by FISMA, since each audit focuses on a sample, or at facilities that previously performed poorly.

The OIG conducted this inspection to determine whether the VA Financial Services Center (FSC) in Austin, Texas, was meeting federal security guidance and focused its inspection on the four security control areas:

1. **Configuration management controls** "identify and manage" security features for all hardware and software components of an information system.[5]
2. **Contingency planning controls** provide reasonable assurance that information resources are protected from unplanned interruptions and their risks minimized, and provide for recovery of critical operations should interruptions occur.[6] Contingency planning also

[1] Federal Information Security Modernization Act (FISMA) Act of 2014, Pub. L. No. 113-283, § 128 (2014).

[2] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, rev. 5, National Institute of Standards and Technology, September 2020, includes updates as of December 10, 2020.

[3] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2020*, Report No. 20-01927-104, April 29, 2021.

[4] Appendix B presents background information on federal information security requirements.

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

[6] GAO, FISCAM.

includes physical and environmental controls, such as fire protection, water damage protection, and emergency power and lighting.

3. **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 the procedures."[7]
4. **Access controls** 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.[8]

What the Inspection Found

Within configuration management, the inspection team identified deficiencies with component inventory, vulnerability management, and flaw remediation. The team did not identify deficiencies with contingency planning controls. The team's review of security management controls identified a deficiency with system and information integrity procedures. Finally, the team identified access control deficiencies in system audit and video surveillance controls.

Configuration Management Controls Had Deficiencies

According to the Government Accountability Office's (GAO) *Federal Information System Controls Audit Manual*, configuration management identifies and controls IT hardware and software security features. The FSC had security deficiencies in the following configuration management controls:

1. **Component inventory,** which is a descriptive record of IT assets in an organization down to the system level.
2. **Vulnerability management,** which is the process by which the Office of Information and Technology (OIT) identifies, classifies, and reduces weaknesses.
3. **Flaw remediation,** which is the process by which organizations correct software defects and which often includes system updates, such as security patches.[9]

The FSC did not have accurate inventories, and this led to other security management control deficiencies. A complete, accurate, and up-to-date inventory is required to implement an

[7] GAO, FISCAM.

[8] Appendix C describes the inspection's scope and methodology.

[9] NIST, "Guide for Security-Focused Configuration Management of Information Systems," *NIST Special Publication 800-128*, Department of Commerce, August 2011; VA Handbook 6500, *Risk Management Framework for VA Information Systems–Tier 3: VA Information Security Program*, March 2015.

effective security program.[10] Inaccurate component inventories affect vulnerability and patch management effectiveness.

As for vulnerability management, OIT scans for vulnerabilities routinely, randomly, or when new vulnerabilities are identified and reported.[11] Although the inspection team and OIT used the same vulnerability-scanning tools, OIT did not detect all vulnerabilities identified by the team. Some of the vulnerabilities were present on multiple computers. The inspection team found OIT did not detect 228 of the 252 vulnerabilities, with 28 considered critical and 200 as high severity.

Due to the vulnerabilities not identified, the inspection team determined that OIT's standard vulnerability identification process and scans were ineffective. The poor component inventories and vulnerability management contributed to inadequate flaw remediation. Despite VA's significant patch management measures, the OIG inspection team identified several devices that were missing patches. Without these controls, VA may be placing critical systems at unnecessary risk of unauthorized access, alteration, or destruction.

No Deficiencies Were Identified for Contingency Planning Controls

During its inspection of the FSC, the inspection team did not identify significant findings in the controls implemented for contingency planning, other than a minor delay in reviewing policies. The FSC is required to review and update these policies on an annual basis. However, the policies expired during the inspection period. The team notified FSC staff and newly signed policies were provided. Deficient controls can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information.[12]

Security Management Controls Had Deficiencies

The OIG team identified one deficiency in security management during its inspection of the FSC. Security management controls establish a framework and continuous cycle for assessing risk, developing security procedures, and monitoring the effectiveness of the procedures. Specifically, system and information integrity procedures provide assurance that the information being accessed has not been meddled with or damaged by an error in the system.

The FSC did not have procedures for how to maintain systems and information integrity. Procedures are detailed steps to be followed to accomplish particular security-related tasks and offer more detail for implementing security policies, standards, and guidelines. When asked about local procedures, a system administrator replied that "procedures do not exist" and staff rely on their education and teachings. Additionally, management does not have a mechanism to

[10] GAO, FISCAM.

[11] VA Handbook 6500.

[12] GAO, FISCAM.

notify users of new policies and procedures or when changes are made. Without procedures, staff may not know how to apply policies or be held accountable for their failure to do so.

Access Controls Had Deficiencies

During its inspection of the FSC, the team identified two deficiencies in access controls. Access controls provide reasonable assurance that computer resources are restricted to authorized individuals and ensure that users have the proper access and are uniquely identified. The following access controls were deficient:

1. **Audit and monitoring controls** involve the collection, review, and analysis of events for indication of inappropriate or unusual activity. These controls should be routinely used to assess the effectiveness of other security controls, recognize an attack, and perform an investigation during or after an attack.
2. **Physical security controls** restrict access to computer resources and protect 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.

Analysis of log data received from the VA Cyber Security Operations Center indicated that 107 of the 278 FSC systems failed to generate or forward audit logs for analysis. Additionally, some VA environments within the FSC-specific network segments provided no audit data in the six-month period reviewed.[13] The inability to generate audit records prevents the collection of audit events, which in turn minimizes VA's ability to review, analyze, and report inappropriate or suspicious activity occurring on the FSC network.

During facility walk-throughs, the inspection team discovered that the FSC's video surveillance system was not fully functional. Before the inspection, the FSC identified that the system was no longer supported by the manufacturer and required updating. Moreover, the FSC infrastructure required a complete upgrade to support the system update. This upgrade was started in early 2019 but was stopped before completion. Subsequently, the video surveillance system contract was canceled. From September 2019 until January 2021, all camera monitoring was performed in real time, and by the end of January 2021, all FSC monitoring cameras were completely offline.[14] In February 2021, a new contract was approved to finish upgrading the system, which the FSC estimated would be completed in August 2021.

[13] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, rev. 5, National Institute of Standards and Technology, September 2020. An environment is the physical, technical, and organizational setting in which an information system operates.

[14] "Real time" indicates the FSC was unable to recall surveillance or produce playback.

Ineffective monitoring and recording of facility activities supporting information systems minimizes the FSC's incident response capabilities. A lack of an effective incident response capability can undermine management's awareness of security vulnerabilities that could hinder the operation of mission-critical systems.

What the OIG Recommended

The OIG recommended the director of VA's FSC (1) implement more effective automated inventory management tools; (2) implement a more effective patch and vulnerability management program that can accurately identify vulnerabilities and enforce patch application; (3) create 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; (4) 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; and (5) continue upgrading the facility's video surveillance system.

VA Comments and OIG Response

The assistant secretary for information and technology and chief information officer provided comments for OIT. OIT concurred with recommendations 1, 3, 4, and 5 and requested recommendation 5 be closed, as corrective actions were completed.

OIT nonconcurred with recommendation 2 to implement a more effective patch and vulnerability management program to accurately identify vulnerabilities and enforce patch application. OIT stated that it was able to demonstrate vulnerability identification, remediation, mitigation, and management rates that indicate VA's vulnerability policies, program, and processes are effective and fall well within acceptable levels, as defined by federal and VA standards.

As a threshold matter, there are no federal standards identifying acceptable levels of vulnerabilities. Moreover, OIT's demonstration of its vulnerability management program occurred after the inspection team conducted scanning and included the results of these scans. In contrast, the OIT scan results, delivered four days prior to the OIG's site visit, did not identify 28 of the critical and 200 of the high-severity vulnerabilities identified by the inspection team. Based on the number of vulnerabilities not identified by OIT, the OIG disagrees that the vulnerability management program is effective. The OIG's conclusion is based on known vulnerabilities that were not mitigated within timeframes established by OIT. OIT also did not provide evidence of a VA standard that defines acceptable vulnerability levels. Accordingly, the OIG stands by its recommendation and recommendation 2 remains open.

OIT provided responsive actions plans for the four recommendations with which it concurred. Based on evidence provided by the FSC, the OIG considers recommendation 5 closed. Appendix D contains the full text of the assistant secretary's response. The OIG will monitor implementation of planned actions and close the open recommendations when VA provides sufficient evidence demonstrating progress in addressing the recommendations and the issues identified.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

Contents

Abbreviations

FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Modernization Act
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

The VA Office of Inspector General (OIG) conducted this inspection to determine whether the VA Financial Services Center (FSC) in Austin, Texas, was meeting federal security requirements and complying with related guidance.[15] Security inspections assess the effectiveness of information technology (IT) controls that protect VA systems and data from unauthorized access, use, modification, or destruction. In 2020, the OIG started an IT security inspection program to provide recommendations to VA on enhancing information security oversight at local and regional facilities. This was the IT inspection program's first inspection in 2021.[16]

The Federal Information Security Modernization Act of 2014 (FISMA) was established, in part, to improve oversight of federal agency information security programs.[17] In accordance with the act, VA must develop, document, and implement an agencywide information security program. FISMA also requires the chief information officers and other senior agency officials to report annually on the effectiveness of the agency's information security program. In addition, FISMA states that inspectors general are required to conduct annual independent evaluations of their respective agencies' information security programs.

The OIG IT inspection program reviews sites not evaluated under the annual FISMA audits (as only a sample of facilities are examined) or facilities that did not perform well in prior FISMA audits. The inspection team selected the VA FSC in Austin, Texas, because of the risk associated with its systems and because one of its applications was involved in a data breach where unauthorized users diverted payments to community healthcare providers during fiscal year (FY) 2020. The application was taken offline.

The OIG's IT inspections are not intended to duplicate the OIG's FISMA audits. However, there is some redundancy in that some of the controls are assessed for both, due to overlapping roles and responsibilities among VA's local, regional, and national facilities and offices. The IT inspections are focused on four security control areas that apply to local facilities and have been selected based on their level of risk (table 1).

[15] Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. No. 113-283, (2014); National Institute of Standards and Technology guidance; VA's IT security policies.

[16] The OIG provided VA with a memorandum related to this inspection containing "VA Sensitive Data" as defined in 38 U.S.C. § 5727. Federal laws, including FISMA, require 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.

[17] FISMA of 2014. See appendix B for additional information about FISMA.

Table 1. Security Controls Evaluated in This Report

Security control area	Definition	Example of controls evaluated
Configuration management controls	"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
Contingency planning controls	Provide reasonable assurance that information resources are protected and risk of unplanned interruptions is minimized, as well as provide for recovery of critical operations should interruptions occur	Continuity of operations, contingency planning, disaster recovery, environmental and maintenance
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 the procedures"	Security awareness, risk management, assessment, authorization, personnel security, and monitoring
Access controls	Provide reasonable assurance that computer resources are restricted to authorized individuals	Access, 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 result in the disruption, destruction, or malicious control of personal information belonging to patients, dependents, beneficiaries, VA employees, contractors, or volunteers.

Security Controls

Both the Office of Management and Budget and the National Institute of Standards and Technology (NIST) provide criteria to evaluate security controls. These criteria provide specific requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system.[18]

According to VA Handbook 6500, the responsibility for developing and maintaining information security policies, procedures, and control techniques lies with the assistant secretary for IT, who is also VA's chief information officer. VA guidance provides the risk-based process for selecting

[18] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, rev. 4, National Institute of Standards and Technology, April 2013, includes updates as of January 22, 2015.

system security controls, including the operational requirements.[19] VA established guidance outlining both NIST and VA-specific requirements to help information system owners select the appropriate controls to secure their systems.

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). OIT delivers available, adaptable, secure, and cost-effective technology services to VA and acts as a steward for VA's IT assets and resources. The Cybersecurity Operations Center is part of OIT's Office of Information Security. It is responsible for protecting VA information and information systems by identifying and reporting emerging and imminent threats and vulnerabilities. OIT has three offices involved in local information security practices:

- **Solution Delivery:** Personnel manage configuration requirements at the national level to help implement configuration management policies and controls. Solution Delivery also establishes configuration baselines for products. Finally, Solution Delivery employs automated mechanisms to centrally manage and verify configuration settings for information system components, such as laptops, workstations, databases, and servers.
- **Patch and Vulnerability Team:** This team distributes information regarding threats and vulnerabilities, as well as available solutions—which could include applying patches. In accordance with the Patch and Vulnerability Team's procedures, OIT uses automated patch management tools across its enterprise to speed up the distribution of patches to systems.[20] The team is organized and maintained by the deputy chief information officer for service delivery, as well as engineering and information systems owners.
- **End User Operations:** Staff execute local systems implementation and engage with VA customers across the nation to meet IT support needs. End User Operations provides on-site and remote support to IT customers. These local site personnel also correct systems issues that cannot be centrally automated.

Figure 1 shows the organizational structure of the entities relevant to this inspection.

[19] VA Handbook 6500, Risk Management Framework for VA Information Systems–Tier 3: VA Information Security Program, March 2015.

[20] VA Handbook 6500.

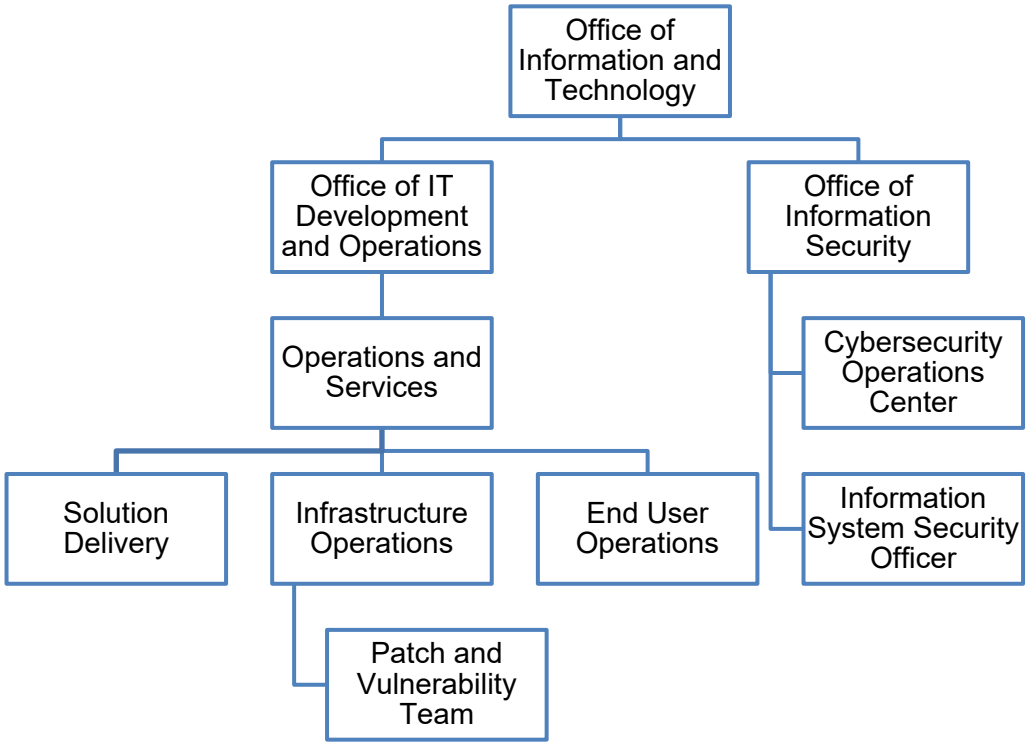

Figure 1. *Organizational structure of entities relevant to this inspection.*
Source: VA OIG analysis.

Prior OIG FISMA Audit

The OIG issues annual reports on VA's information security program based on audits conducted by an independent public accounting firm, CliftonLarsonAllen LLP. The FY 2020 FISMA audit included an evaluation of 48 major applications and general support systems hosted at 24 VA facilities, including the testing of selected management, technical, and operational controls outlined by NIST.[21] CliftonLarsonAllen LLP made 26 recommendations, listed in appendix A. Twenty-three are repeat recommendations from the prior annual audit, indicating that VA continues to face significant challenges in complying with FISMA.[22] The FSC was evaluated during the FY 2018 FISMA audit, when deficiencies were identified in configuration

[21] Office of Management and Budget, Circular A-130, app. III, "Security of Federal Automated Information Resources," November 28, 2000. The circular's appendix defines a general support system as an interconnected set of information resources under the same direct management control which shares common functionality.

[22] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2020,* Report No. 20-01927-104. April 29, 2021. Appendix B presents information about FISMA and other federal criteria and standards discussed in this report.

management, security management, and access controls. However, the inspection team did not identify repeat findings during this inspection.

Related Government Accountability Office Review

A November 2019 Government Accountability Office (GAO) testimony found that VA was one of the federal agencies that continued to have a deficient information security program.[23] According to GAO, VA faced several security challenges as it secured and modernized its information systems:

- effectively implementing information security controls
- mitigating known vulnerabilities
- establishing elements of its cybersecurity risk management program
- identifying critical cybersecurity staffing needs
- 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 risk of disruption."[24]

VA Financial Services Center

The FSC (shown in figure 2) is a VA franchise fund (fee-for-service) organization that offers a wide range of financial and accounting products and services to both VA and other government agencies.[25] FSC services are organized around revenue centers and product lines to better focus service delivery and accountability.

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

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

[25] Under the authority of the Government Management Reform Act of 1994 and the Military Quality of Life and Veterans Affairs Appropriations Act, 2006, Public Law 109-114.

Figure 2. *The VA Financial Services Center.*
Source: Department of Homeland Security, Facility Security Assessment, January 29, 2021.

Results and Recommendations

The inspection team reviewed configuration management, contingency planning, security management, and access controls at the VA FSC. Within configuration management, the team identified deficiencies with component inventory, vulnerability management, and flaw remediation.

While evaluating the contingency planning controls, the inspection team did not identify deficiencies with associated policies, plans, training, testing, alternate storage and processing, system backups, recovery, preventative maintenance, or environmental controls.

The inspection team's review of security management controls focused on the security program, assessment and validation of risk, control implementation, awareness and personnel security, monitoring, remediation, and third-party security. The inspection team identified a deficiency with system and information integrity procedures.

Finally, the inspection team reviewed access controls that include boundary protection, sensitive resources, physical security, system audit, identification, authentication, and authorization. The inspection team identified deficiencies in system audit and video surveillance controls.

Configuration Management Controls

According to the GAO's *Federal Information System Controls Audit Manual* (*FISCAM*), configuration management identifies and controls IT hardware and software security features.[26] The inspection team reviewed 24 configuration management controls for VA-hosted systems (drawn from NIST criteria) at the VA FSC to determine if they met federal guidance and VA requirements. 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 activities performed to define, track, store, manage, and retrieve configuration items. Examples of these controls are baseline configurations, configuration settings, and component inventories.

[26] GAO, *FISCAM*.

- **Authorize, test, approve, and track changes** by formally establishing a change management process, with management's authorization and approval of the changes and including documentation and approval of test plans, comprehensive and appropriate testing of changes, and 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.[27] 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 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 emergency changes and have them approved** by appropriate entity officials. In addition, 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.

To achieve effective configuration management, VA must first establish an accurate component inventory to identify all computers on the network. Component inventories affect the success of other controls like vulnerability and patch management. OIT's Cybersecurity Operations Center identifies and reports threats and vulnerabilities for VA. Once this process is complete, OIT's Patch and Vulnerability Team develops procedures for remediation that address identified issues and can include applying patches. This process helps secure computers from attack.

The OIG's IT inspections also include a review of locally hosted systems. These systems may include minor applications that, if not part of a general support system, require some level of protection.[28] As the inspection team did not identify any locally hosted systems at the FSC, these

[27] 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.

[28] Committee on National Security Systems, "Committee on National Security Systems Glossary."

controls were not evaluated. The FSC's general support system controls were inherited from VA's general support system and assessed in the annual FISMA audits.

Finding 1: Configuration Management Controls Had Deficiencies

To assess configuration management controls, the inspection team interviewed information system security officers, local administrators, and local configuration control management and system stewards. The team observed system change management processes; reviewed local policies, procedures, and inventory lists; and scanned the FSC's network to identify devices. The team also received vulnerability lists from OIT and scanned the FSC's network to identify vulnerabilities.[29] A comparison of the OIT and team scans showed that VA did not

- identify all the devices in the FSC's network;
- identify all critical or high-risk vulnerabilities in the network; or
- remediate flaws, including unsupported versions of applications, missing patches, and vulnerable plug-ins.

The inspection team found that VA's policies and procedures addressed control criteria, such as establishing a configuration management plan, controlling baseline configurations, and implementing a change control process. However, by not implementing more effective inventory management controls, VA is placing critical systems at unnecessary risk of unauthorized access, alteration, or destruction.

Component Inventory

Previous FISMA reports have repeatedly identified inventory deficiencies as a nationwide issue for VA. Component inventories are descriptive records of IT assets in an organization, down to the system level. A complete, accurate, and up-to-date inventory is required to implement an effective information security program because it provides greater visibility into and control over these systems.[30] A comprehensive view of the components improves a security program by identifying what needs to be managed and secured. The inspection team identified inaccuracies in the component inventory at the FSC, despite OIT and VA's use of automated systems to maintain a readily available baseline of its information systems. VA identified 466 devices in the FSC's inventory; the inspection team, however, identified 1,252 devices.

[29] See appendix C for additional information about the inspection's scope and methodology.
[30] GAO, *FISCAM*.

Vulnerability Management

Prior FISMA audits repeatedly found deficiencies in VA's vulnerability assessments. Consistent with those findings, the team identified weaknesses in vulnerability management at the FSC. 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 FSC's vulnerability management controls did not effectively identify weaknesses in its network. For example, the inspection team identified unsupported versions of applications, missing patches, and noncurrent antivirus signatures.[31] Unsupported applications receive no new security patches and may contain security vulnerabilities. Devices missing patches contain known vulnerabilities that the patches are intended to correct. Antivirus applications are most effective when they are fully up to date, and the latest signatures improve malware detection.

NIST assigns severity levels to vulnerabilities by using the Common Vulnerability Scoring System, a framework for communicating the characteristics of software vulnerabilities.[32] The scoring system provides a way to capture the principal characteristics of a vulnerability and produces a numerical score reflecting its severity. Numerical scores are classified as risk levels such as low, medium, high, or critical to help organizations properly assess and prioritize their vulnerability management processes. For example, on a scale of zero to 10, critical vulnerabilities have a score between 9.0 and 10, while high-risk vulnerabilities have a score between 7.0 and 8.9. OIT establishes time frames for remediating vulnerabilities based on their severity.

OIT provided network vulnerability scan results from the FSC to the inspection team on February 18, 2021. The team conducted scans of the same network from February 22 through March 4, 2021. The team and OIT used the same vulnerability-scanning tools. The team identified 252 vulnerabilities—32 critical vulnerabilities on 122 computers and 220 high-risk vulnerabilities on 222 computers—that were not mitigated within the OIT-established time frames. The team identified vulnerabilities such as operating systems that are no longer supported and applications with missing patches. Unsupported operating systems may become less secure over time as vendors no longer release updates and patches to remedy emerging vulnerabilities. Missing patches can expose systems to security and functionality problems. Some vulnerabilities were present on multiple computers. As seen in figure 3, the team found 28 vulnerabilities scored as critical and 200 as high severity that OIT did not detect.

---

[31] NIST, "Guide to Malware Incident Prevention and Handling for Desktops and Laptops," *NIST Special Publication 800-83,* rev. 1, Department of Commerce, July 2013. A signature is a set of characteristics of known malware instances that can be used to identify known malware and some new variants of known malware.

[32] "Vulnerability Metrics," NIST, accessed August 17, 2021, 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 (FIRST), accessed July 8, 2021, https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf.

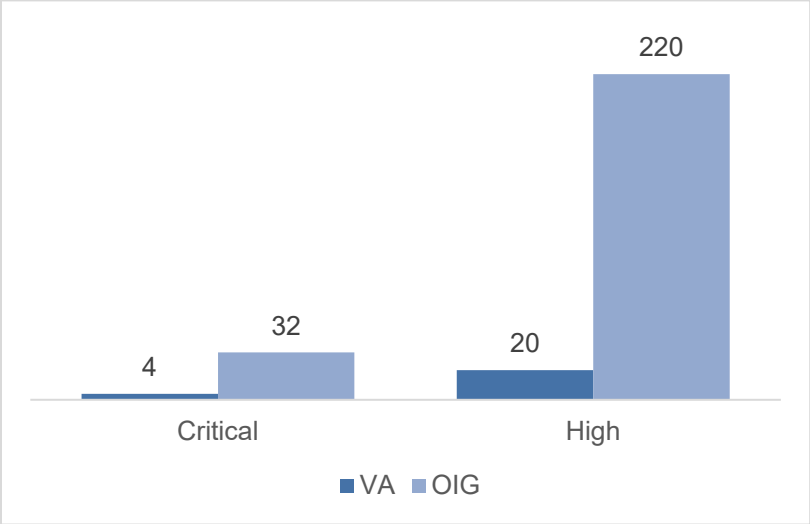

Figure 3. *Vulnerabilities identified by VA and the OIG inspection team. Source: VA OIG analysis.*

The Cybersecurity Operations Center identifies and reports threats and vulnerabilities for VA. In addition, OIT conducts scans for vulnerabilities routinely, randomly, or when new vulnerabilities are identified and reported.[33] However, due to the vulnerabilities that OIT did not identify, the inspection team determined that the scans were inadequate.

According to GAO, "Vulnerability assessments involve analyzing a network to identify potential vulnerabilities that would allow unauthorized access to network resources, simulating what might be performed by someone trying to obtain unauthorized access."[34] Unidentified threats cannot be mitigated; they represent weaknesses that could be exploited to gain access to VA data. Management personnel, therefore, should periodically perform assessments to protect information, address vulnerabilities, and make decisions about accepting or mitigating risks.[35]

Flaw Remediation

The FSC did not remediate all flaws for devices in its network. The inspection team identified unsupported versions of applications, missing patches, and vulnerable plug-ins. When an application is unsupported, the product may have security vulnerabilities. In addition, no new security patches will be created. Devices missing patches contain known vulnerabilities that the

[33] VA Handbook 6500. Appendix B provides additional information about federal criteria and standards discussed in this report.

[34] Committee on National Security, CNSSI No. 4009: A vulnerability is a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source."

[35] NIST, "Managing Information Risk," *NIST Special Publication 800-39*, Department of Commerce, March 2011. "Organizations can accept risk deemed to be low, moderate, or high depending on particular situations or conditions. Organizations typically make determinations regarding the general level of acceptable risk and the types of acceptable risk with consideration of organizational priorities."

patches are intended to correct. If patches are not applied, the vulnerabilities will continue to exist. Attackers can also exploit vulnerable plug-ins in web browsers.[36]

Flaw remediation is the process by which organizations correct software defects, including applying updates such as patches.[37] Patches are usually the most effective way to mitigate software flaw vulnerabilities and are often the only fully effective solution. According to GAO, a patch is a piece of software code that is inserted into a program to temporarily fix a defect until an updated version is released. 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. Although patch management is a critical process used to help alleviate many of the challenges involved with securing systems from cyberattack, previous FISMA audits have repeatedly found deficiencies in this area.[38]

The Infrastructure Operations Security Management Office established a permanent enterprise patch and vulnerability program in June 2017. The program identifies, remediates, and mitigates vulnerabilities. OIT uses automated patch management tools across its enterprise to speed up the distribution of patches to systems in accordance with the Patch and Vulnerability Team's procedures.[39] The team distributes information regarding threats and vulnerabilities as well as available solutions, which can include applying patches. If patches cannot be applied using automated tools, a notification is sent to End User Operations technicians to apply patches and update systems.

Despite VA's significant patch management measures, the inspection team identified several devices that were missing patches. For example, several web servers were missing patches for critical and high-risk vulnerabilities. Web servers publish information to the internet and are the most often targeted and attacked hosts on an organization's network.[40] Without an effective patch management program, vulnerabilities such as security and functionality problems in software and firmware might not be mitigated, increasing opportunities for exploitation.

---

[36] NIST, "Security Guide for Interconnecting Information Technology Systems," *NIST Special Publication 800-47*, Department of Commerce, August 2002. A vulnerability is "a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy."

[37] VA Handbook 6500.

[38] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2020*, Report No. 20-01927-104, March 31, 2020.

[39] VA Handbook 6500.

[40] *Committee on National Security Systems (CNSS) Glossary*, CNSSI No. 4009, April 6, 2015. A host is "any hardware device that has the capability of permitting access to a network via a user interface, specialized software, network address, protocol stack, or any other means. Some examples include, but are not limited to, computers, personal electronic devices, thin clients, and multi-functional devices."

Finding 1 Conclusion

The FSC did not have accurate inventories, which led to critical and high-severity vulnerabilities in the systems not being detected or remediated. Inaccurate inventories and ineffective vulnerability assessments prevented an effective patch management program, which is required to remediate flaws in VA systems within time frames determined by OIT.

Recommendations 1–2

The OIG made the following recommendations to the Financial Services Center director:

1. Implement measures to maintain an accurate system inventory.
2. Implement a more effective patch and vulnerability management program that can accurately identify vulnerabilities and enforce patch application.

Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendation 1. The assistant secretary reported OIT is working to improve FSC's physical inventory compliance.

The assistant secretary nonconcurred with recommendation 2. The assistant secretary reported that during the inspection OIT was able to demonstrate vulnerability identification, remediation, mitigation, and management rates that indicate VA's vulnerability policies, program, and processes are effective, falling well within acceptable levels as defined by federal and VA standards.

OIG Response

While the assistant secretary indicated the corrective actions regarding recommendation 1 were to be completed in December 2021, OIT did not provide evidence that action had been completed or request that the OIG close the recommendation. The OIG will monitor implementation of planned actions and close the recommendation when VA provides sufficient evidence demonstrating progress.

As a threshold matter, there are no federal standards identifying acceptable levels of vulnerabilities. The fact of what vulnerabilities were identified and when they were identified is crucial. OIT's demonstration of its vulnerability management program was provided after the OIG conducted scanning at the FSC. The OIG provided the results of its scans to OIT shortly after concluding the scans. OIT stated that it input these scan results into the vulnerability management program. In contrast, OIT's own scan results, delivered four days prior to the OIG's site visit, did not identify 28 of the critical and 200 of the high-severity vulnerabilities identified by the inspection team. Due to the number of vulnerabilities not identified by OIT, the OIG disagrees that their vulnerability management program is effective. The OIG's conclusion is

based on known vulnerabilities that were not mitigated within timeframes established by OIT. OIT also did not provide evidence of a VA standard that defines acceptable vulnerability levels. Accordingly, the OIG stands by its recommendation. The full text of the response from the assistant secretary is included in appendix D.

Contingency Planning Controls

Contingency planning for systems is part of an overall program for achieving continuity of operations for organizational mission and business functions. According to FISCAM, contingency planning controls provide reasonable assurance that controls are in place to protect information resources, minimize the risk of unplanned interruptions, and provide recovery of critical operations should interruptions occur. Elements of effective contingency planning include

- assessment of the criticality and sensitivity of computerized operations and identification of supporting resources;
- steps taken to prevent and minimize potential damage and interruption;
- establishment of a comprehensive contingency plan; and
- periodic testing of the contingency plan, with appropriate adjustments based on testing.[41]

If contingency planning controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. To determine whether recovery plans will work as intended, they should be tested periodically in disaster-simulation exercises. FISMA requires that each federal agency implement an information security program that includes "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency." Although often referred to as disaster recovery or contingency plans, controls to ensure service continuity should address the entire range of potential disruptions. These may include minor interruptions, such as temporary power failures, as well as disasters, such as fires, natural disasters, and terrorism, which would require reestablishing operations at a remote location.

To determine if the FSC met federal guidance and VA requirements, the inspection team evaluated 47 contingency planning controls in the following categories:

- **Contingency plans, policies, and procedures** formally establish the authority and guidance necessary to develop an effective contingency plan. Contingency plans contain detailed guidance and procedures for restoring damaged systems unique to the systems' security impact level and recovery requirements.
- **Contingency training and testing** validate recovery capabilities and prepare recovery personnel for plan activation.

[41] GAO, *FISCAM*.

- **Alternate storage and processing sites** are geographically distinct from primary storage sites and maintain duplicate copies of information and data if the primary storage site is not available. Similarly, alternate processing sites provide processing capability if the primary processing site is not available.
- **System backup, recovery, and reconstitution** ensure that backup information is adequate to ensure the confidentiality, integrity, and availability of the backup data. System recovery is the ability to execute contingency plan activities to restore organizational mission or business functions. Reconstitution takes place following recovery for returning systems to fully operational states.
- **Preventative maintenance** helps mitigate equipment failure or malfunction and restores operating capability within approved time frames that follow manufacturer specifications or organizational requirements.
- **Environmental controls** prevent damage or interruptions in service (including activities such as maintaining fire suppression systems, smoke or water detectors, redundant cooling systems, and backup power supplies).

The inspection team did not identify deficiencies with the maintenance or environmental security controls at the FSC. The team retrieved and reviewed local contingency plans, policies, standard operating procedures, and other applicable VA policies. The team also interviewed the continuity of operations program manager, disaster recovery and preparedness manager, information system security officer, regional contracting officer representatives, system stewards, local administrators, and account manager personnel. Additionally, the team conducted walk-throughs of IT rooms, mail rooms, and workspaces.

The inspection team made the following observations:

- Local plans, policies, and procedures contained the required information on risks and operational priorities, critical applications and restoration priorities, training requirements for contingency personnel, contingency plan exercises, roles and responsibilities, alternate recovery locations, storage, and backup.
- Environmental controls were in place to ensure IT equipment maintained proper temperature and humidity and to provide for emergencies such as fire detection and suppression, and loss of power.

Finding 2: No Deficiencies Were Identified for Contingency Planning Controls

During its inspection of the FSC, the inspection team did not identify significant findings in the controls implemented for contingency planning. The team did find that some policies expired

during the review. The FSC is required to review and update these policies on an annual basis. The team notified FSC staff and newly signed policies were provided.

The FSC's existing plans, policies, and procedures addressed threats, vulnerabilities, risks, activation plans, personnel notification, deactivation and recovery operations, testing, training, and exercising of plans. The inspection team verified the FSC had an alternate storage and processing facility, and there was evidence that training and testing were conducted in accordance with policies. The team also identified evidence of system backup, recovery, and reconstitution. Maintenance and environmental controls were in place and documented. As the team did not identify any deficiencies in the FSC's contingency planning controls other than the minor lapse in updating policies, the OIG did not make any recommendations.

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 seven critical security management controls:

- **Institute a security management program** that establishes policies, plans, and procedures clearly describing all major systems and facilities and 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 undertaking a comprehensive identification and consideration of all threats and vulnerabilities. This step ensures that the greatest risks are addressed and that appropriate decisions are made regarding which risks to accept or which to mitigate. 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 management.
- **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 effectiveness of the program** to ensure that policies and controls are effective to reduce risk on an ongoing basis. Effective monitoring involves performing tests of 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, application of appropriate corrective actions, and follow-up monitoring to make sure actions are effective. Plans of actions and milestones are developed to track weaknesses and corresponding corrective actions.

- **Ensure third parties are secure,** as they are often granted access to systems for purposes such as outsourced software development and system transactions for vendors, business partners, and contractors.[42]

During its inspection, the team reviewed local security management policies, standard operating procedures, and applicable VA policies. These included documentation from the Enterprise Mission Assurance Support Service, which is VA's cybersecurity management service for workflow automation and continuous monitoring. The team also conducted interviews with the information system security officers, local administrators, contracting officer's representatives, human resources staff, privacy officers, and system stewards.

Finding 3: Security Management Controls Had Deficiencies

The FSC established a security management program and assessed and validated risk. It also implemented security awareness and personnel policies as required and ensured third parties were secure.

The FSC's local policies contained the required information, and processes were in place for onboarding and termination of VA employees and contractors. However, the FSC did not have procedures for maintaining systems and information integrity.

Systems and Information Integrity Procedures

The FSC did not have procedures for maintaining systems and information integrity. These procedures would include information such as who is responsible for managing network segments and how they report that information for inclusion in Cybersecurity Operations Center scanning. Examples of system and information integrity controls are flaw remediation, malicious code protection, security function and verification, input validation, error handling, and memory protection.

Scanning is required to validate the integrity of a system and identify vulnerabilities that could affect system and information integrity. Integrity involves guarding against improper modification or destruction and includes ensuring information authenticity. System and information integrity provide assurance that the information being accessed has not been meddled with or damaged by an error in the system.

Procedures provide detailed steps regarding how to implement security policy standards and guidelines. While manuals may mix policy and procedures, to be effective tools they must clearly distinguish between policy and implementation. Procedures are established at the

[42] GAO, *FISCAM*.

business process and system levels, describing how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure.

When asked about local procedures, a system administrator told the inspection team that procedures do not exist and staff rely on their education and training. Management does not have a mechanism to notify users of new or updated policies and procedures. Without procedures, staff may not know how to apply policies, and managers cannot hold them accountable for failing to do so.

Finding 3 Conclusion

Although the FSC issued required policies about system and information integrity, it did not create the necessary procedures detailing how to apply them to local systems. Until the FSC develops local procedures, staff may not know how to properly apply security controls to local systems, placing VA at risk of loss of confidentiality, integrity, and availability of VA information.

Recommendation 3

The OIG made the following recommendation to the Financial Services Center director:

3. Implement systems 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.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with the recommendation and stated that the FSC is improving communication at all levels to ensure policies are being applied effectively, with an estimated completion date of February 2022.

OIG Response

The assistant secretary's planned corrective actions are responsive to the intent of the recommendation. The OIG will monitor implementation of the planned actions and will close the recommendation when VA provides sufficient evidence demonstrating progress in addressing the issues identified. The full text of the response from the assistant secretary is included in appendix D.

Access Controls

Access controls, including boundary protections, sensitive system resources, physical security, audit, and monitoring provide reasonable assurance that computer resources are restricted to authorized individuals. Identification, authentication, and authorization controls ensure that users have the proper access and are uniquely identified.

At the FSC, the inspection team reviewed all six critical access control elements:

- **Boundary protection controls** pertain to the protection of a logical or physical boundary around a set of information resources and implementing measures to prevent unauthorized information exchange across the boundary. Firewall devices represent 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, recognize an attack, and 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.

To assess these controls, the inspection team conducted interviews with the information system security officers, local administrators, contracting officer's representatives, human resources staff, privacy officers, and physical security personnel. During walk-throughs, the team inspected the physical security controls at the facility.

Finding 4: Audit, Monitoring, and Physical Security Access Controls Had Deficiencies

To evaluate FSC's access controls, the inspection team interviewed the information system security officers, system stewards, local administrators, and the system owner; reviewed local policies and procedures; conducted walk-throughs of the facility; and analyzed audit logs.[43] The team determined that

- systems at the FSC failed to generate or forward audit reports to the Cybersecurity Operations Center for analysis, and
- the video surveillance system was inoperable.

Audit and Monitoring

Previous FISMA reports have repeatedly identified access controls as a nationwide issue for VA. The inspection team identified weaknesses in FSC's audit and monitoring controls after it reviewed policies and procedures, interviewed appropriate personnel, and reviewed a sample of log data from October 2020 through March 2021. The FSC's existing policies and procedures addressed auditable events and responsible parties. However, analysis of log data received from the Cybersecurity Operations Center indicated that 107 of 278 FSC systems failed to generate or forward audit logs to the Cybersecurity Operations Center for analysis, as required by local policy. Specifically, all FSC systems using two-server operating systems either failed to generate or forward audit data to the Cybersecurity Operations Center. Additionally, some VA environments within FSC-specific network segments provided no audit data in the six-month period reviewed.[44]

The inability to generate audit records prevents the collection of audit events, minimizing VA's ability to review, analyze, and report inappropriate or suspicious activity occurring on the FSC network.

Physical Security: Video Surveillance

During the facility walk-throughs, the inspection team discovered that the FSC's physical access control system was not fully functional, as the video surveillance system was not operational. In 2019, the FSC learned that the system was no longer supported by the manufacturer and required updating. However, the FSC infrastructure required a complete system upgrade to support the surveillance system upgrade. The FSC began the upgrade in early 2019 but stopped in September 2019 before completion. Then the FSC physical access control system contract was

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

[44] According to NIST, an environment is the physical surroundings in which an information system processes, stores, and transmits information.

canceled. From September 2019 until January 2021, all camera monitoring was real time only.[45] By the end of January 2021, all monitoring cameras in the FSC were completely offline. In February 2021, a new contract was approved to finish upgrading the system, with estimated completion in August 2021.

Ineffective monitoring and recording of facility activities in and around information systems minimizes incident response capabilities of the security force. The lack of an effective incident response can undermine management's awareness of security vulnerabilities that could hinder the operation of mission-critical systems.

Finding 4 Conclusion

The FSC is not generating or forwarding audit reports for many of its systems, minimizing VA's ability to review, analyze, and report inappropriate or suspicious activity in the network. Additionally, the FSC has not had a fully functional video surveillance system since September 2019, reducing personnel's ability to respond to security threats.

Recommendations 4–5

The OIG made the following recommendations to the Financial Services Center director:

4. In conjunction with the system owner, develop and implement capabilities for all systems to generate audit logs and collect and forward audit events to the Cybersecurity Operations Center for review, analysis, and reporting.
5. Continue to upgrade the video surveillance system and ensure new capabilities provide full surveillance and video retention to improve monitoring and incident response.

Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 4 and 5. The assistant secretary reported that VA has implemented an enterprise-wide visibility to all end points, regardless of their event logging status. Visibility includes, but is not limited to, asset inventory, asset vulnerability posture, and asset network communication. The data of these technologies and capabilities feed into the enterprise logging solution.[46]

The assistant secretary also stated that the FSC completed the video surveillance upgrade in October 2021 and requested removal or closure of the video surveillance findings.

[45] "Real time" indicates the FSC was unable to recall surveillance or produce playback.

[46] While the assistant secretary's response did not include an expected implementation date for corrective actions in response to recommendation 4, the deputy chief information officer for quality, performance, and risk reported to the OIG on January 19, 2022, that its target implementation date was January 31, 2022.

OIG Response

The corrective actions reported by the assistant secretary are responsive to the intent of the recommendations. Based on evidence provided by the FSC, the OIG considers recommendation 5 closed. The OIG will monitor implementation of the actions in response to recommendation 4 and will close the recommendation when VA provides sufficient evidence demonstrating progress in addressing the issues identified. The full text of the response from the assistant secretary is included in appendix D.

Conclusion

The IT security inspection program was started in 2020 to provide recommendations to enhance IT oversight at local facilities. The FSC was the first site the OIG inspected in 2021. The inspection team identified deficiencies in configuration and security management as well as in access controls related to component inventory, vulnerability management, flaw remediation, system auditing, and video surveillance. The OIG made five recommendations to the FSC director: (1) implement more effective automated inventory management tools; (2) implement a more effective patch and vulnerability management program that can accurately identify vulnerabilities and enforce patch application; (3) create 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; (4) 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; and (5) continue upgrading the facility's video surveillance system. The team did not identify any deficiencies in the remaining areas evaluated.

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

Appendix A: FISMA Audit for Fiscal Year 2020 Report Recommendations

In the FISMA audit for FY 2020, CliftonLarsonAllen LLP made 26 recommendations. Of these, 23 were repeat recommendations from the prior year. The only new recommendations were 9, 10, and 19. The FISMA audit assesses the agencywide security management program, and recommendations in the FISMA report are not specific to the FSC. The full list of recommendations follows:

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 documents such as security plans and interconnection agreements on an annual basis and ensure the information 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.
9. Strengthen processes to ensure appropriate levels of background investigations are completed for applicable VA employees and contractors and applicable investigation data is accurately tracked within the authoritative system of record.

10. Formalize the position descriptions and methodology used within the human resource business processes to ensure that employees with similar positions are required to have the same level of background investigation.
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 implemented 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. Consolidate the security responsibilities for networks not managed by the Office of Information and Technology, under a common control for each site and ensure vulnerabilities are remediated in a timely manner.
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 integrate 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 are 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 VA's Cybersecurity Operations Center has full access to all security incident data to facilitate an 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. Fully develop a comprehensive list of approved and unapproved software and implement continuous monitoring processes to prevent the use of prohibited software on agency devices.
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 GAO developed FISCAM to provide auditors and information system control specialists with 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 NIST controls.

Federal Information Security Modernization Act of 2014

The stated goals of FISMA follow:

- 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.[47]

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 OIG accomplishes the annual FISMA evaluation through a contracted external auditor and provides oversight of the contractor's performance.

[47] FISMA.

NIST Information Security Guidelines

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

Appendix C: Scope and Methodology

Scope

The inspection team conducted its work from January 2021 through September 2021. When the team inspected the FSC during the week of February 22, 2021, the facility was largely vacant, with most employees teleworking. Due to COVID-19 restrictions, the team maintained social distance from the FSC staff who were present and followed the Centers for Disease Control and Prevention's recommendations, including wearing masks. To further limit contact with FSC personnel, the team conducted most interviews remotely. The team evaluated configuration management, contingency planning, security management, and access controls of operational VA IT assets and resources in accordance with VA's IT security policy, FISMA, and NIST security guidelines. In addition, the team assessed the capabilities and effectiveness of IT 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 conducted interviews of VA personnel responsible for FSC IT security and operations, privacy compliance, and human resources 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 IT 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.[48] The team obtained an understanding of relevant internal controls, then assessed and evaluated the controls applicable to the inspected site.

[48] VA Handbook 6500.

In planning the inspection, the OIG team identified GAO's *Standards for Internal Control in the Federal Government* components significant to the objectives. The inspection team determined that all controls applicable to the FSC aligned with one of the following categories: control environment, control activities, information and communication, and monitoring. 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 inspection.

Data Reliability

The inspection team generated computer-processed data by using network scanning tools. The results of the scans were provided to the 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, 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.

In addition, computer-processed data included reports from the IBM QRADAR system that VA used to collect audit log data from FSC systems. In this process, the team was not testing VA data or systems for transactional accuracy. The team used this data to identify systems sending data from FSC to QRADAR. To test for reliability, the team determined whether any data were missing from key fields or were outside the timeframe requested. The review team also assessed whether the data contained obvious duplication of records, alphabetic or numeric characters in incorrect fields, or illogical relationships among data elements. Testing of the data disclosed that they were sufficiently reliable for the review objectives.

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: January 12, 2022

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

Subj: OIG Draft Report, Inspection of Information Technology Security at the VA Financial Services Center, (Project No. 2021-01221-AE-0049)

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

Thank you for the opportunity to review the Office of Inspector General (OIG) draft report, "*Inspection of Information Technology Security at the VA Financial Services Center*." The Office of Information and Technology submits the attached written comments.

(Original signed by)

The OIG removed point of contact information prior to publication.

Kurt DelBene

Attachment

005 Attachment

Office of Information and Technology

Comments on OIG Draft Report,

Inspection of Information Technology Security at the VA Financial Service Center

(OIG Project No. 2021-01221-AE-0049)

OIG Recommendation 1:

The OIG recommends the Financial Services Center Director implement measures to maintain an accurate system inventory.

Comments: Concur. VA OIT is working to improve FSC's physical inventory compliance and is tracking for full compliance by December 2021.

OIG Recommendation 2:

The OIG recommends the Financial Services Center director implement a more effective patch and vulnerability management program that can accurately identify vulnerabilities and enforce patch application.

Comments: Non Concur: VA OIT non concurs with OIGs findings and recommendations related to vulnerability management and flaw remediation. Within the timeframe of the overall inspection, VA OIT was able to demonstrate vulnerability identification, remediation, mitigation, and management rates that indicate VA's vulnerability policies, program, and processes are effective, falling well within acceptable levels, as defined by federal and VA standards.

OIG Recommendation 3:

The OIG recommends the Financial Services Center director implement systems 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.

Comments: Concur. FSC is improving communication to all levels to ensure policies are being applied effectively. Estimated completion date: February 2022.

OIG Recommendation 4:

The OIG recommends the Financial Services Center director in conjunction with the system owner, develop and implement capabilities for all systems to generate audit logs and collect and forward audit events to the Cybersecurity Operations Center for review, analysis, and reporting.

Comments: Concur. The VA has implemented an Enterprise wide visibility to all end points regardless of their event logging status. Visibility includes, but is not limited to, asset inventory, asset vulnerability posture and asset network communication. The data of these technologies/capabilities feed into the enterprise logging solution.

OIG Recommendation 5:

The OIG recommends the Financial Services Center director continue to upgrade the video surveillance system and ensure new capabilities provide full surveillance and video retention to improve monitoring and incident response capabilities.

Comments: Concur. FSC completed the video surveillance upgrade. Completion date was October 2021. VA OIT requests removal or closure of the Video Surveillance findings.

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/Audit/Review Team	Mike Bowman, Director Luis Alicea Tom Greenwell Jack Henserling Shawn Hill Adam Sowells
Other Contributors	Kathy Berrada Christopher Dong

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

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