US DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS HEALTH ADMINISTRATION

Follow-Up Information Security Inspection at the Southwest Consolidated Mail Order Pharmacy in Tucson, Arizona

Information Security Inspection	**23-03721-180**	**September 5, 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, and destruction. To determine compliance with the Federal Information Security Modernization Act (FISMA) of 2014, 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.

The fiscal year 2023 FISMA audit indicated that VA continues to face significant challenges meeting the law's requirements. The audit made 25 recommendations to VA. Repeat recommendations included addressing deficiencies in configuration management, contingency planning, security management, and access controls.[2] 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 four control areas the OIG determined to be at highest risk.[3] Typically, facilities selected for these inspections either were not included in the annual audit sample or had previously performed poorly. The OIG conducted this follow-up inspection to determine whether the systems at the Southwest Consolidated Mail Order Pharmacy (CMOP) in Tucson, Arizona, were meeting federal security guidance. The OIG previously inspected the Southwest CMOP in 2021 and made six recommendations to correct identified security weaknesses.[4]

During this follow-up inspection, the team identified continuing significant deficiencies related to configuration management and access controls designed to protect systems at the Southwest CMOP from unauthorized access, alteration, and destruction. VA's Office of Information and Technology (OIT) was in the process of implementing an enterprise-wide solution to address prior OIG findings in these two areas and had not completed it at the time of the site visit. The OIG initially notified OIT of both deficiencies in June 2022, and the resulting remediation plans had not been fully implemented more than two years later. Table 2 in the Results and Recommendations section of this report summarizes findings and recommendations from the

[1] Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. §§ 3551–3558; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2023*, Report No. 23-01105-69, May 14, 2024.

[2] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2023*, Report No. 23-01105-69, May 14, 2024.

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

[4] VA OIG, *Inspection of Information Technology Security at the Consolidated Mail Outpatient Pharmacy in Tucson, Arizona*, Report No. 21-02453-99, June 1, 2022.

initial Southwest CMOP information security inspection and whether facility managers had implemented effective controls to address prior recommendations. The inspection scope and methodology are described in appendix C.

The OIG's inspections are focused on 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, minimize risk, and provide for recovery of critical operations should interruptions occur.[6]
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 these procedures."[7]
4. **Access controls** provide reasonable assurance that computer resources are restricted to authorized individuals. These controls include access, identification, authentication, audit, and accountability, including physical security controls.[8]

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

What the Follow-Up Inspection Found

The OIG identified continued deficiencies with configuration management controls, security management controls, and access controls. The inspection team did not identify any deficiencies in contingency planning.

Configuration Management Controls Had Two Deficiencies

The Southwest CMOP had deficiencies in two configuration management controls:

- **Vulnerability remediation:** Analysis of the OIT vulnerability scan results and plans of action and milestones indicated that the facility did not create plans of action and milestones for vulnerabilities that were not remediated within established time frames.

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

[6] GAO, *FISCAM*.

[7] GAO, *FISCAM*.

[8] GAO, *FISCAM*.

- **System life-cycle management:** The OIG team found that CMOP's network devices and servers were running software that was not securely configured.

Vulnerability Remediation

As of October 2023, the Southwest CMOP had eight critical-severity vulnerabilities on 357 hosts, which are network systems and devices, and 62 high-severity vulnerabilities on 481 hosts that had not been mitigated within the timelines established by OIT. Of these unmitigated vulnerabilities, two of the critical-severity vulnerabilities and 49 of the high-severity vulnerabilities did not have plans of action and milestones created to define corrective actions in response to the identified security risks. A similar deficiency was noted during the prior inspection of the Southwest CMOP.

System Life-Cycle Management

The inspection team noted that all 52 of the Southwest CMOP's network devices had software that did not meet baseline security requirements.[9] Further, 57 of 65 servers (88 percent) did not meet baseline security requirements. Specifically, the CMOP did not use current security baselines to configure the network devices and servers. In accordance with VA policy, these network devices should have received vendor-issued updates as part of the standard system development life-cycle process.[10] Furthermore, systems should use baseline configurations that have been documented, formally reviewed, and agreed upon by management. Baseline configurations serve as a basis against which to measure future changes to systems that include the implementation of security and privacy controls. The baseline configurations for the network equipment are established by the OIT Configuration Control Board. Network devices and information technology systems are a part of VA's most critical infrastructure. Applying vendor-issued updates is not just a defensive strategy but a proactive one that helps protect network stability.

The Southwest CMOP Had One Deficiency in Security Management Controls for Account Management

The Southwest CMOP had a deficiency related to management of user accounts for terminated employees. Account management is the process of requesting, establishing, issuing, and closing user accounts; tracking users and their respective access authorizations; and managing these functions.[11]

[9] These network devices include switches and a router to control network traffic.

[10] VA's Developments, Security and Operations Information System Vulnerability Management Plan, Version 1.0, March 28, 2022.

[11] NIST Special Publication 800-53.

The Southwest CMOP needs to ensure administrator accounts are disabled when employment is terminated. Specifically, the inspection team determined that an administrator account was still active five months after the user's employment was terminated. A review of the account indicated that it was used after the termination. CMOP personnel indicated that this account required a physical token that was managed by a security system and that the token was destroyed when the individual resigned. Further, CMOP personnel indicated that the account's continued activity was the result of the security system validating the account. However, the OIG could not confirm this.

Access Controls Had Two Deficiencies

Access controls provide reasonable assurance that computer resources are restricted to authorized individuals. The Southwest CMOP had deficiencies in the following access controls:

- **Network segmentation** regulates where information can travel within and between systems.[12]
- **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 investigate during or after an attack.[13]

Network segmentation

The Southwest CMOP did not have network segmentation controls in place for four special-purpose system segments.[14] Network-connected special-purpose systems are placed on isolated network segments for protection, which is provided through access control lists. However, the OIG identified four network segments containing 50 special-purpose system devices that did not have access control lists applied. Without network segmentation controls in place, any user can access these systems, which run potentially vulnerable special-purpose devices.

Audit and Monitoring

The OIG determined that improvements are needed for logging administrative actions, log retention, and log reviews for databases at the facility. These controls should be routinely used to assess the effectiveness of other security controls, recognize an attack, and investigate during or

[12] NIST Special Publication 800-53.

[13] NIST Special Publication 800-53.

[14] The VA's Specialized Device Isolation Architecture Guidance (SDIAG) Version 1.2, September 8, 2017, recommends the use of network segmentation as a means to accomplish boundary protection for special purpose systems.

after an attack.[15] The Southwest CMOP had not deployed mechanisms to copy database log files to long-term storage devices or prevent logs from being overwritten. Logs frequently help with investigating security incidents and performing subsequent analysis. They 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 understanding the unauthorized use or modification of information.

The Southwest CMOP did not segregate all special-purpose system networks, and database audit logs were not properly retained. Unless the CMOP takes corrective actions, it risks unauthorized access to critical network resources, inability to respond effectively to incidents, and loss of personally identifiable information.

What the OIG Recommended

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

1. Improve vulnerability management processes to ensure plans of action and milestones are created for vulnerabilities that cannot be mitigated within OIT timelines.
2. Implement a more effective system life-cycle process to ensure network devices are running operating systems that are configured to approved baselines and are free of vulnerabilities.
3. Implement a process to verify that when employees are terminated, all their accounts are disabled.
4. Ensure network segmentation controls are applied to all network segments with special-purpose systems.

The OIG's fifth recommendation, which is similar to a recommendation made during the prior inspection, is addressed to the director of the Southwest Consolidated Mail Order Pharmacy, in conjunction with the assistant secretary for information and technology:

5. Implement a process to retain database logs for a period consistent with VA's record retention policy.

VA Management Comments and OIG Response

The assistant secretary for information and technology and chief information officer concurred with recommendations 1, 3, and 5. In response to recommendation 2, the assistant secretary concurred in part, noting that some discrepancies were the result of false positives. The assistant secretary stated that VA remediated and closed all issues. As a result, the assistant secretary

[15] NIST Special Publication 800-53.

requested recommendations 1, 2, 3, and 5, be closed due to corrective actions he said were completed. VA did not concur with recommendation 4.

Regarding recommendation 1, the assistant secretary provided evidence and requested closure of the recommendation; however, the corrective actions do not fully address the OIG's findings regarding vulnerability remediation. The process OIT developed to link identified vulnerabilities to plans of actions and milestones, discussed in this report, constitutes only a first step toward correcting the deficiency. Results are inconclusive and do not yet demonstrate that this new process will work as intended. When VA can demonstrate that the plan of action and milestones process effectively mitigates security risks for unremedied security vulnerabilities, recommendation 1 will be closed.

In response to recommendation 2, the assistant secretary concurred in part, noting that some discrepancies were the result of false positives. Regarding recommendation 3, the assistant secretary reported that the Southwest CMOP updated user accounts to comply with VA regulations. For recommendation 5, the assistant secretary indicated that the Infrastructure Operations, Platforms Support, and Database Management Service Line implemented processes to retain database logs. The OIG determined that the planned corrective actions are responsive to the intent of recommendations 2, 3, and 5, and the assistant secretary provided sufficient evidence to support that actions to address these recommendations were completed. The OIG considers these recommendations closed.

The assistant secretary for information and technology responded that VA did not concur with recommendation 4, stating that the VA's approach to network segmentation is consistent with VA policy. After reviewing the pertinent guidance, the OIG maintains that not segmenting special purpose systems is inconsistent with VA guidance on this topic.[16] That guidance states that the agency will restrict access to segments that contain Special Purpose Systems or place the Special Purpose Systems in a standalone network.

During the inspection, OIT representatives stated that an authorizing official accepted the risk of not applying access control lists to the Special Purpose Systems network segments because these segments are subject to the VA's vulnerability remediation processes. The OIG team reviewed OIT's June 2024 scan results of the Special Purpose Systems network segments and found that no critical or high vulnerabilities existed on these network segments for more than one month. While the scan results demonstrated that existing scanning processes mitigated inherent risks to Special Purpose Systems devices on the network for the month reviewed, OIT would benefit from following VA guidance to ensure adequate protection of such devices. The OIG will consider closing this recommendation when OIT can demonstrate that existing scanning processes result in an effective and sustained mitigation strategy against inherent risks and the

[16] VA's Specialized Device Isolation Architecture Guidance (SDIAG) Version 1.2, September 8, 2017.

Authorizing Official explicitly accepts the risk of not implementing network segmentation of the Special Purpose Systems.

The full text of the assistant secretary's response is included in appendix D.

Larry M. Reinkemeyer

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

Contents

Abbreviations

CMOP	Consolidated Mail Order Pharmacy
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
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 (FISMA) of 2014, 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.[17] The FISMA audit is conducted in accordance with guidelines issued by the Office of Management and Budget (OMB) and applicable National Institute of Standards and Technology (NIST) information security guidelines.

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, and destruction. Appendix B presents information about FISMA and other federal criteria and standards discussed in this report. Typically, facilities selected for these inspections either were not included in the annual FISMA sample or had previously performed poorly. Inspections provide recommendations to VA on enhancing information security oversight at local and regional facilities.[18] Appendix C provides more detail on the inspection's scope and methodology.

The OIG previously inspected the Southwest Consolidated Mail Order Pharmacy (CMOP) in Tucson, Arizona, in 2021 and made six recommendations to correct identified security weaknesses.[19] During this follow-up information security inspection, the team reviewed configuration management, contingency planning, security management, and access controls at the Southwest CMOP to determine if VA had taken appropriate corrective actions.

[17] Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. §§ 3551–3558; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2023*, Report No. 23-01105-69, May 14, 2024.

[18] 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 ability to accomplish its mission.

[19] VA OIG, *Inspection of Information Technology Security at the Consolidated Mail Outpatient Pharmacy in Tucson, Arizona*, Report No. 21-02453-99, June 1, 2022.

Security Controls

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

The 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.[21] In addition, VA Handbook 6500 describes the risk-based process for selecting system security controls, including the operational requirements.[22] VA established guidance outlining both NIST- and VA-specific requirements to help information system owners select the appropriate controls to secure their systems.

This information security inspection focused on four security control areas that were covered in the prior inspection and selected based on their level of risk, as shown in table 1.

[20] 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*, Security and Privacy Controls for Federal Information Systems and Organizations*, September 23, 2021.

[21] 38 USC 5723(b).

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

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
Contingency planning	Provide reasonable assurance that information resources are protected, and the 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 controls, and flaw remediation
Security management	Ensure continuous and effective risk assessment, including developing, implementing, and monitoring the effectiveness of security procedures	Risk management, assessment, authorization, and monitoring
Access	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 disrupt access to, destroy, or allow malicious control of personal information belonging to patients, dependents, beneficiaries, VA employees, or contractors.

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 solution delivery process.

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

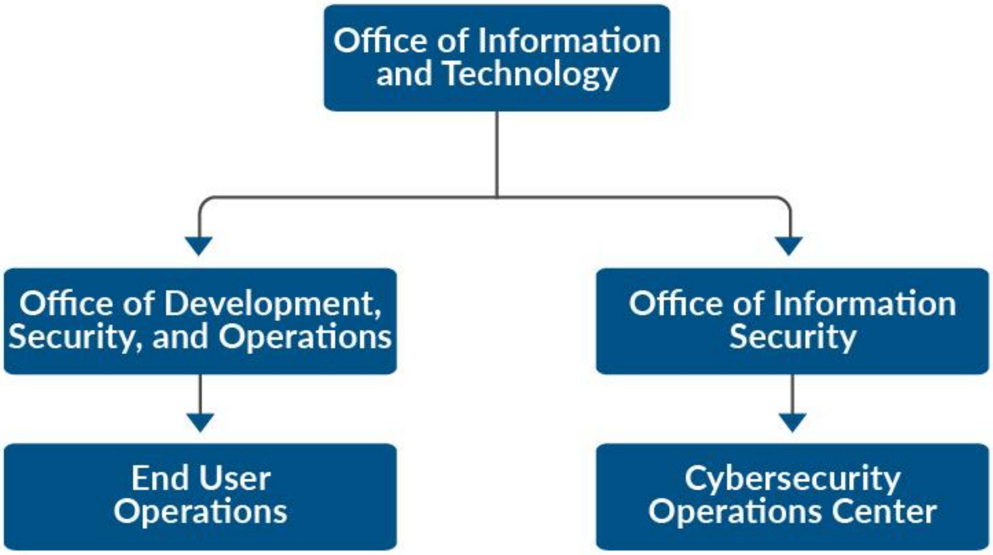
Office of Information and Technology
Office of Development, Security, and Operations
Office of Information Security
End User Operations
Cybersecurity Operations Center

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

End User Operations provides on-site and remote support to information technology (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. Information Technology Operations and Services 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 infrastructure operations services' personnel to the Southwest CMOP, 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 OMB and applicable NIST information security guidelines.[23] The fiscal year (FY) 2023 FISMA audit, conducted by independent public accounting firm CliftonLarsonAllen LLP, evaluated 45 major applications and general support systems hosted at 23 VA facilities, including the testing of selected

[23] 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; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2023*, Report No. 23-01105-69, May 14, 2024. Appendix A details the FISMA audit's recommendations.

management, technical, and operational controls outlined by NIST.[24] CliftonLarsonAllen LLP made 25 recommendations, listed in appendix A. All 25 recommendations are repeated from the prior annual audit, indicating that VA continues to face significant challenges in complying with FISMA requirements.[25] Repeat recommendations included addressing deficiencies in configuration management, security management, and access controls.

The OIG previously inspected the Southwest CMOP in 2021 and made six recommendations to correct identified security weaknesses. During the follow-up information security inspection in 2023, the team reviewed configuration management, security management, contingency planning, and access controls to determine if VA had 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.[26] According to GAO, VA faced several security challenges while securing and modernizing its information systems, including

- effectively implementing information security controls,
- mitigating known vulnerabilities,
- 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 systems will remain at risk of disruption."[27]

Southwest CMOP

An OIT representative indicated the Pharmacy Benefits Management Services operates VA's seven CMOPs, including the Southwest CMOP in Tucson (shown in figure 2). Combined, the VA CMOPs processed almost 131 million prescriptions in FY 2023. Approximately 86 percent of Veterans Health Administration outpatient prescriptions are filled by the CMOPs. The CMOPs also fill prescriptions for 74 Indian Health Service sites and the VA Civilian Health and

[24] OMB, Circular A-130, app. 3, "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 that share common functionality.

[25] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2023*. Appendix B presents information about FISMA and other federal criteria and standards discussed in this report.

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

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

Medical Program. The Southwest CMOP facility is approximately 80,000 square feet and is located on 4.55 acres. The Southwest CMOP's annual budget is $1.1 billion, and it processed almost 22.8 million prescriptions in FY 2023. VA medical sites in Alaska, Arizona, California, Colorado, Hawaii, Idaho, Oregon, New Mexico, Nevada, Utah, Washington, and Wyoming are assigned to the Southwest CMOP.

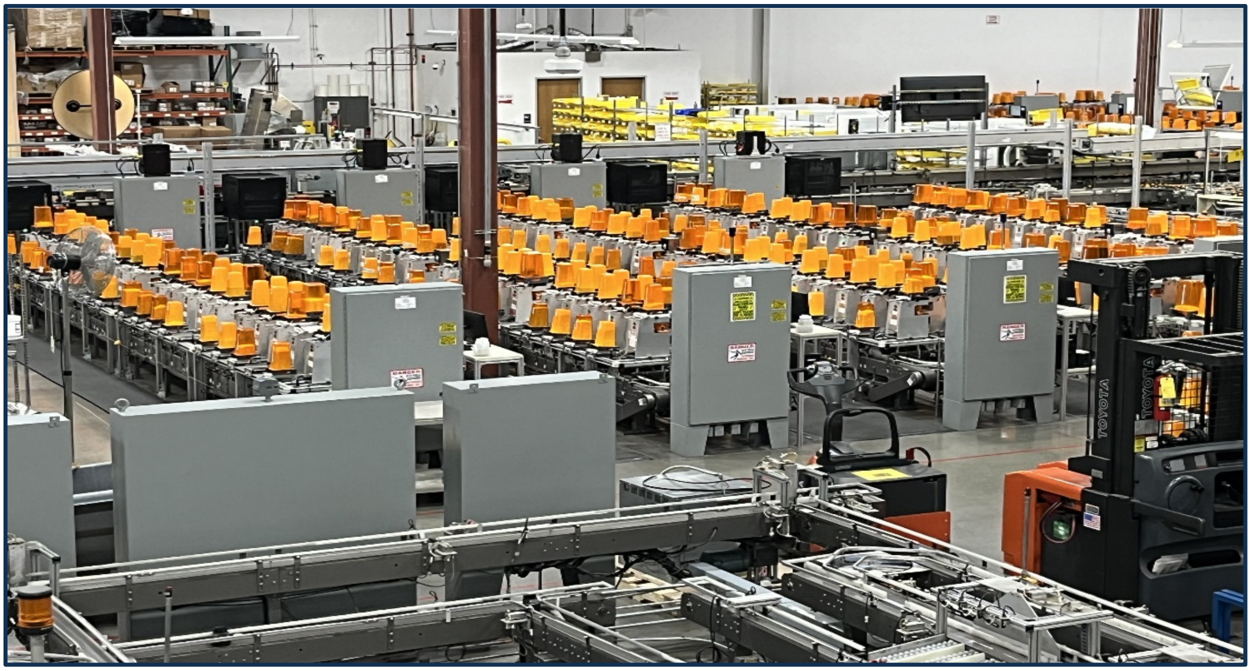

Figure 2. *A portion of the Southwest CMOP production floor, where prescriptions are filled.*
Source: Southwest CMOP information system security officer.

Results and Recommendations

The inspection team reviewed configuration management, contingency planning, security management, and access controls at the Southwest CMOP. The team evaluated these controls during the follow-up information security inspection in 2023 because the OIG determined the areas to be at highest risk of not adequately protecting veterans' sensitive data hosted at the Southwest CMOP. While contingency planning had improved, the follow-up inspection continued to identify deficiencies related to configuration management, security management controls, and access controls. Table 2 summarizes the findings and recommendations from the prior inspection and shows whether facility management implemented effective controls to address prior recommendations or if the problems persisted, resulting in repeat findings in FY 2023.

Table 2. Evaluation of Actions Addressing Prior Recommendations

Control area	Prior finding	Prior recommendation	Repeat finding in FY 2023?
Configuration management	The Southwest CMOP did not have accurate asset inventories.	Implement more effective inventory management tools for all network segments.	No
	The Southwest CMOP did not identify and remediate all critical or high vulnerabilities in the network.	Implement a more effective vulnerability and flaw remediation program that can accurately identify vulnerabilities and enforce flaw remediation.	Yes
	The Southwest CMOP did not fully implement the CMOP configuration management plans.	Develop and implement methods to ensure delivery, receipt, and understanding of assigned roles and responsibilities for CMOP activities to ensure full implementation of approved policy.	No
Contingency planning	The Southwest CMOP has not developed or put into place disaster recovery plans as required by VA authorization procedures.	Develop and implement a disaster recovery plan and capability that will restore operations in the event of a disruption to critical operations.	No
Access	The CMOP's video surveillance system utilized default passwords.	Task the facility manager to change the default username and password for the security camera system.	No
	Southwest CMOP systems failed to generate or forward audit logs for analysis.	Configure audit logging on the misconfigured devices in accordance with established baselines, policy, and procedures.	Yes

Source: VA OIG analysis.

While the CMOP has matured its configuration management processes to address some deficiencies, the OIG identified repeat security weaknesses related to vulnerability remediation processes designed to protect sensitive information at the CMOP. Additionally, the CMOP faces challenges with unsupported infrastructure components.

During the OIG's review of security management controls, the team identified a recurring deficiency with user account management. Specifically, the team noted that an administrator account was not disabled when the employee left the CMOP.

Finally, the review of access controls continued to identify deficiencies in network segregation, as well as in audit and monitoring controls. 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 systems was not corrected, and management has not made progress implementing automated tools for managing access controls. Specifically, the OIG identified a lack of database audit logging at the facility, demonstrating that the CMOP's audit and monitoring controls still need improvement.

I. Configuration Management Controls

According to 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 critical configuration management 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. VA should first establish an accurate component inventory to identify all devices on the network.[28] 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.

[28] GAO, *FISCAM*.

Finding 1: The Southwest CMOP Had Deficiencies in Two Configuration Management Controls

To assess configuration management controls, the inspection team interviewed the area manager, information system security officer, and local IT specialists. The team reviewed local policies, procedures, and inventory lists and scanned the Southwest CMOP's network to identify devices. The team compared the devices found on the network with the device inventories provided by VA, evaluated vulnerability lists provided by OIT, and scanned the network to identify vulnerabilities and check for compliance with baseline configurations.[29] The team also conducted a walk-through of the facility.

The team concluded that the Southwest CMOP had deficiencies in two configuration management controls:

- **Vulnerability remediation.** Analysis of the OIT vulnerability scan results and plans of action and milestones indicated that the facility did not create plans of action and milestones for vulnerabilities that were not remediated within established time frames.
- **System life-cycle management.** The OIG team found that CMOP's network devices and servers were running software that was not securely configured.

Vulnerability Remediation

VA has a vulnerability management program, but it can be improved. This is a repeat finding from the last inspection. Prior FISMA audits repeatedly found deficiencies in VA's vulnerability management controls. Consistent with those findings, the team identified deficient controls at the Southwest CMOP.[30] 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. Since the prior inspection, OIT has implemented a formal process to track the monitoring and remediation of vulnerabilities by using a plan of action and milestones vulnerability portal. However, this process has not demonstrated that it will effectively remediate security vulnerabilities within organizational timelines. The OIG also notes that the repeat vulnerability management finding was initially

[29] OIT imports its vulnerability scan results into the Information Central Analytics and Metrics Platform for reporting vulnerabilities to system owners. See appendix C for additional information about the inspection's scope and methodology.

[30] 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."

communicated to OIT in June 2022 and the resulting remediation plan had not been fully implemented more than two years later.

VA conducts periodic independent scans of all its systems. Discovered vulnerabilities are entered into a plan of action and milestones for remediation by the information 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.[31]

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 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 that critical-severity vulnerabilities be remediated within 30 days and high-severity vulnerabilities be remediated in 60 days.[33]

The inspection team compared OIT-provided network vulnerability scan results from the Southwest CMOP against OIG scans conducted from October 16 through October 19, 2023. The team and OIT used the same vulnerability scanning tools. As of October 2023, the Southwest CMOP had eight critical vulnerabilities on 357 hosts, which are network systems and devices, and 62 high vulnerabilities on 481 hosts that had not been mitigated within the timelines, established by OIT. Of these unmitigated vulnerabilities, two critical and 49 high vulnerabilities did not have plans of action and milestones laying out corrective actions. A similar deficiency was noted during the prior inspection of the Southwest CMOP, and the OIG made a recommendation that had still not been fully implemented during the follow-up inspection.

[31] Per the NIST SP 800-37, Rev 2, an information 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.

[32] "Vulnerability Metrics," NIST National Vulnerability Database, accessed August 7, 2023, https://nvd.nist.gov/vuln-metrics/cvss; "Common Vulnerability Scoring System ver. 3.1, 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.

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

System Life-Cycle Management

The inspection team noted that all 52 of the Southwest CMOP's network devices used software that did not meet baseline security requirements.[34] Further, 57 of 65 servers (88 percent) did not meet baseline security requirements. In accordance with VA policy, network devices should have received vendor-issued updates as part of the standard system development life-cycle process, but at the CMOP, they did not.[35] Furthermore, systems should use baseline configurations that have been documented, formally reviewed, and agreed upon by management. Baseline configurations serve as a basis for measurement against future changes to systems that include the implementation of security and privacy controls.[36] Baseline configurations for network equipment are established by the VA OIT Configuration Control Board. Network devices and IT systems are VA's most critical infrastructure. Applying vendor-issued updates is not just a defensive strategy but a proactive one that helps protect network stability.

Finding 1 Conclusion

System vulnerabilities were not always mitigated within OIT-established timelines, and software did not meet baseline requirements. These vulnerabilities created security weaknesses on the CMOP's network that could be exploited by malicious individuals to gain unauthorized access to sensitive information or disrupt operations.

Recommendations 1–2

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

1. Improve vulnerability management processes to ensure plans of action and milestones are created for vulnerabilities that cannot be mitigated within Office of Information and Technology timelines.
2. Implement a more effective system life-cycle process to ensure network devices are running operating systems that are configured to approved baselines and free of vulnerabilities.

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

[34] These network devices include switches and a router to control network traffic.

[35] VA's Development, Security and Operations Information System Vulnerability Management Plan, Version 1.0, March 28, 2022.

[36] NIST Special Publication 800-53.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 1 and 2, and requested these recommendations be closed due to corrective actions he said were completed. For recommendation 1, the assistant secretary indicated that OIT improved the vulnerability management process and remediated the vulnerabilities the OIG identified. In response to recommendation 2, the assistant secretary concurred in part, noting that some discrepancies were the result of false positives. The assistant secretary stated that VA remediated and closed all issues. The full text of the assistant secretary's response is included in appendix D.

OIG Response

Regarding recommendation 1, the assistant secretary provided evidence and requested closure of the recommendation; however, the corrective actions do not fully address the OIG's findings regarding vulnerability remediation. The process OIT developed to link identified vulnerabilities to plans of actions and milestones, discussed in this report, constitutes only a first step toward correcting the deficiency. Results are inconclusive and do not yet demonstrate that this new process will work as intended. When VA can demonstrate that the plan of action and milestones process effectively mitigates security risks for unremedied security vulnerabilities, recommendation 1 will be closed.

The planned corrective actions are responsive to the intent of recommendation 2, and the assistant secretary provided sufficient evidence to support that actions taken were completed. The OIG considers this recommendation closed.

II. Contingency Planning Controls

"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."[37] To determine whether recovery plans will work as intended, they should be tested periodically in disaster simulation exercises.[38] 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."[39] Although often referred to as disaster recovery or contingency plans, controls to ensure service continuity should address the entire range of potential disruptions.[40] These may include minor interruptions, such as temporary power failures, as well as fires, natural disasters, and terrorism, which would require reestablishing operations at a remote location. To determine if the facility met federal guidance and VA requirements, the inspection team evaluated five contingency planning controls.[41]

Finding 2: The Southwest CMOP Had No Contingency Planning Control Deficiencies

To assess contingency planning controls, the inspection team interviewed the area manager; information system security officer; members of OIT's Office of Development, Security, and Operations; and facility management. The team also reviewed local policies and procedures.

The OIG found that VA's policies and procedures addressed control criteria such as identifying critical operations and performing preventive maintenance. The team verified that the site's information system contingency plan established comprehensive procedures to recover the facility's IT operations quickly and effectively following a service disruption. After the prior inspection of the Southwest CMOP, the facility developed and tested a disaster recovery plan. Furthermore, the facility conducted contingency training, testing, and recovery exercises in accordance with policies. The team did not identify deficiencies in contingency planning controls. Accordingly, the OIG did not make any recommendations for improvement.

[37] GAO, *FISCAM*.

[38] GAO, *FISCAM*.

[39] FISMA § 3554(b)(8).

[40] GAO, *FISCAM*.

[41] The five contingency controls evaluated are continuity of operations, contingency planning, disaster recovery, environmental, and maintenance.

III. 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 critical elements of security management related to user account administration.[42]

Finding 3: The Southwest CMOP Had One Security Management Control Deficiency

To assess security management controls, the inspection team reviewed local security management policies, standard operating procedures, and applicable VA policies, including documentation from the Enterprise Mission Assurance Support Service—VA's cybersecurity management service for workflow automation and continuous monitoring. Among the documents reviewed were the security control policies and procedures, and plans of action and milestones for known deficiencies. The team also interviewed the area manager and information system security officer. Finally, the team conducted a walk-through of the facility. The OIG identified a weakness with account management controls at the Southwest CMOP.[43]

Account Management Controls

The Southwest CMOP needs to ensure administrator accounts are disabled when employment is terminated. Specifically, the inspection team determined that an administrator account was still active five months after the user's employment was terminated, and a review of the account indicated that it was used after the termination. CMOP personnel indicated that this account required a physical token that was managed by a security system and that the token was destroyed when the individual resigned. Further, CMOP personnel indicated that the account's continued activity was the result of the security system validating the account. However, the OIG could not confirm this.

Finding 3 Conclusion

CMOP managers failed to disable an administrative account when an individual left VA employment. The account created security weaknesses because it could have been exploited by malicious individuals to gain unauthorized access to sensitive information or disrupt operations.

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

[43] Per NIST Special Publication 800-53, account management includes creating, enabling, modifying, disabling, and removing user accounts; monitoring users and their respective access authorizations; and managing these functions.

Recommendation 3

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

3. Implement a process to verify that when employees are terminated, all their accounts are disabled.

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

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendation 3 and requested the recommendation be closed due to corrective actions he said were completed. In addition, the assistant secretary reported that the Southwest CMOP updated user accounts. The full text of the assistant secretary's response is included in appendix D.

OIG Response

The planned corrective actions are responsive to the intent of recommendation 3. The assistant secretary provided sufficient evidence to support actions taken in response this recommendation, and the OIG considers the recommendation closed.

IV. 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.[44] Physical access controls involve restricting physical access to computer resources and protecting them from loss or impairment. At the Southwest CMOP, the inspection team reviewed three critical elements: logical access controls, physical access controls, and environmental controls. The Southwest CMOP had a repeat access control finding related to audit and monitoring controls. During the 2023 inspection, OIT was in the process of implementing an enterprise-wide auditing and monitoring solution to address prior OIG findings in this area. However, this process was not yet fully implemented at the Southwest CMOP during the 2023 site visit. The OIG also notes that the repeat auditing and monitoring control finding was initially communicated to OIT in June 2022 and the resulting remediation plan had not been fully implemented more than one year later.

Finding 4: The Southwest CMOP Had Deficiencies in Two Access Controls

To evaluate logical access controls on the CMOP's network, the inspection team reviewed the configuration of network equipment. To evaluate the CMOP's physical access and environmental controls, the inspection team interviewed the area manager, information system security officer, and local IT specialists. The team also reviewed local policies and procedures, conducted walk-throughs of the facility, and analyzed audit logs.[45]

The Southwest CMOP had deficiencies in two access controls:

- **Network segmentation** regulates where information can travel within and between systems.[46]
- **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 investigate during or after an attack.[47]

[44] NIST Special Publication 800-53.

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

[46] NIST Special Publication 800-53.

[47] NIST Special Publication 800-53.

Network Segmentation Controls

The Southwest CMOP did not have network segmentation controls in place for six special-purpose system segments.[48] Network-connected special-purpose systems are placed on isolated network segments for protection, which is provided through access control lists.[49] However, the OIG identified four network segments containing 50 special-purpose system devices that did not have access control lists applied. Without network segmentation controls in place, any user can access these potentially vulnerable special purpose devices.

Audit and Monitoring

The OIG determined that improvements are needed for logging administrative actions, retaining logs, and reviewing logs for databases at the facility. The Southwest CMOP had not deployed mechanisms to copy database log files to a long-term storage device or prevent them from being overwritten. Logs help with investigating security incidents and performing subsequent analysis. They 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 the unauthorized use or modification of information. The OIG noted similar findings and made a recommendation during the prior inspection.

Finding 4 Conclusion

The Southwest CMOP did not segregate all special-purpose system networks, and database audit logs were not properly retained at the facility. Unless the CMOP takes corrective actions, it risks unauthorized access to critical network resources, inability to respond effectively to incidents, and loss of personally identifiable information.

Recommendations 4–5

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

4. Ensure network segmentation controls are applied to all network segments with special-purpose systems.

The OIG also made the following recommendation to the director of the Southwest Consolidated Mail Order Pharmacy and the assistant secretary for information and technology, which is similar to a recommendation that was made during the prior inspection:

[48] The VA's Specialized Device Isolation Architecture Guidance (SDIAG) Version 1.2, September 8, 2017, recommends the use of network segmentation as a means to accomplish boundary protection for special purpose systems.

[49] Access control lists isolate network segments by limiting the resources that can be accessed within them.

5. Implement a process to retain database logs for a period consistent with VA's record retention policy.

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

VA Management Comments

The assistant secretary for information and technology and chief information officer did not concur with recommendation 4, stating that VA is following policies concerning network segmentation. For recommendation 5, the assistant secretary stated that the Infrastructure Operations, Platforms Support, and Database Management Service Line implemented processes to retain database logs. The assistant secretary requested this recommendation be closed due to corrective actions he said were completed. The full text of the assistant secretary's response is included in appendix D.

OIG Response

The assistant secretary for information and technology did not concur with recommendation 4, stating that the VA's approach to network segmentation is consistent with VA policy. Reviewing the pertinent guidance, not segmenting special purpose systems is inconsistent with VA guidance on this topic.[50] That guidance states that the agency will restrict access to segments that contain Special Purpose Systems or place the Special Purpose Systems in a standalone network.

During the inspection, OIT representatives stated that an authorizing official accepted the risk of not applying access control lists to the Special Purpose Systems network segments because these segments are subject to the VA's vulnerability remediation processes. The OIG team reviewed OIT's June 2024 scan results of the Special Purpose Systems network segments and found that there were no critical or high vulnerabilities existed on these network segments for more than one month. While the scan results demonstrated that existing scanning processes mitigated inherent risks to Special Purpose Systems devices on the network for the month reviewed, OIT would benefit from following VA guidance to ensure adequate protection of such devices. The OIG will consider closing this recommendation when OIT can demonstrate that existing scanning processes result in an effective and sustained mitigation strategy against inherent risks and the Authorizing Official explicitly accepts the risk of not implementing network segmentation of the Special Purpose Systems.

[50] VA's Specialized Device Isolation Architecture Guidance (SDIAG) Version 1.2, September 8, 2017.

The planned corrective actions are responsive to the intent of recommendation 5. The assistant secretary provided sufficient evidence to support actions taken, and the OIG considers this recommendation closed.

Appendix A: Federal Information Security Modernization Act (FISMA) of 2014 Audit for FY 2023 Report Recommendations

In the FISMA audit for fiscal year 2023, CliftonLarsonAllen LLP made 25 recommendations.[51] Of these, all 25 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 Southwest Consolidated Mail Order Pharmacy. The 25 recommendations made to the Assistant Secretary for Information and Technology are listed below.

1. 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 a risk-based rotation, or 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 accounts and permissions in excess of required functional responsibilities, and to remove unauthorized or unnecessary accounts.

[51] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2023*, Report No. 23-01105-69, May 14, 2024.

8. Enable system audit logs on all critical systems and platforms and conduct centralized reviews of security violations across the enterprise.
9. Implement improved processes for establishing and maintaining accurate investigation 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 improved processes for tracking and resolving vulnerabilities that cannot be addressed within policy timeframes. Implement more effective patch and vulnerability management processes to mitigate identified security deficiencies and reduce applicable security risks.
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 controls that restrict vulnerable medical devices from unnecessary access to 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. Implement improved procedures to ensure that system outages and disruptions are tracked to specific system boundaries and that interdependent systems are considered for the purposes of tracking and measuring against stated system recovery time objectives.
19. Ensure contingency plans for all systems and applications are updated and tested in accordance with VA requirements.
20. Ensure that systems and applications are adequately logged and monitored to facilitate an agencywide awareness of information security events.

21. Implement improved safeguards to identify and prevent unauthorized vulnerability scans on VA networks.

22. 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.

23. Implement improved processes to monitor for unauthorized changes to system components and the installation of prohibited software on all agency devices and platforms.

24. Develop a comprehensive inventory process to identify connected hardware, software, and firmware used to support VA applications and operations.

25. 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 (FISCAM)

The Government Accountability Office (GAO) developed *FISCAM* to give auditors and information system control specialists a specific methodology for evaluating the confidentiality, integrity, and availability of information systems. *FISCAM* groups 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 identification of other emerging threats. Software releases should be controlled to prevent

[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.

the use of noncurrent software. Examples of these controls are software usage restrictions, user-installed software, 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 performance metrics.[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.

Federal Information Security Modernization Act (FISMA) of 2014

The following are the stated goals of FISMA:

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

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

Appendix C: Scope and Methodology

Scope

The inspection team conducted its work from September 2023 through May 2024. The team evaluated configuration management, contingency planning, 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, and destruction.

Methodology

To accomplish the objective, the inspection team examined relevant laws and policies and inspected the Southwest Consolidated Mail Order Pharmacy (CMOP) and its systems for security compliance. Additionally, the team interviewed VA personnel responsible for the facility's information technology security, operations, and privacy compliance. 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's 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 GAO's *FISCAM* as a template to plan the inspection. When planning for this inspection, the team identified potential information system controls that would significantly affect the review. Specifically, the team used the *FISCAM* appendix II as a guide to help develop evidence requests and interview questions for CMOP personnel. The team used the *FISCAM* controls identified in appendix B of this report to determine the FISMA controls used by VA to protect and secure its information systems. Although similar to the contractor-conducted annual FISMA audits, this review focused on security controls that are implemented at the local level. However, there are some controls that overlap and are included 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 Southwest CMOP are aligned with the control activities category. Control activities are the actions that 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 in 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 Office of Information and Technology Compliance, Readiness, and Remediation team. 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. The team relied on the results of the scanning tool and network device configuration. The team performed its own scans to determine whether the agency scans were complete and accurate, met intended purposes, and were not subject to alteration.

Government Standards

The OIG conducted this review 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: June 11, 2024

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

Subj: Follow-Up Information Security Inspection at the Southwest Consolidated Mail Order Pharmacy in Tucson, Arizona (VIEWS 11715118)

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 Southwest Consolidated Mail Order Pharmacy in Tucson, Arizona*.

2. The Office of Information and Technology (OIT) submits the attached written comments, along with evidence to support closure for each of the OIG's recommendations to the Department.

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 Southwest Consolidated Mail Order Pharmacy in Tucson, Arizona

(VIEWS 11715118)

Recommendation 1: Improve vulnerability management processes to ensure plans of action and milestones are created for vulnerabilities that cannot be mitigated within OIT timelines.

Comments: Concur.

The Department of Veterans Affairs (VA) Office of Information and Technology (OIT) has improved vulnerability management processes, and the vulnerabilities identified by the Office of Inspector General (OIG) have been remediated.

Expected Completion Date: Completed. Completion date: November 1, 2023.

VA requests closure of Recommendation 1.

Recommendation 2: Implement a more effective system life-cycle process to ensure network devices are running operating systems that are configured to approved baselines and are free of vulnerabilities.

Comments: Concur.

VA concurs in part with the findings reported by the OIG. While some false positives derived from default settings, there were also some discrepancies requiring remediation. VA remediated and closed all issues and verified compliance with additional checks. **Expected Completion Date:** Completed. Completion date: February 26, 2024.

VA requests closure of Recommendation 2.

Recommendation 3: Implement a process to verify that when employees are terminated, all their accounts are disabled.

Comments: Concur.

Tucson Consolidated Mail Order Pharmacy local information and technology updated user accounts in compliance with the OIG’s findings and VA regulations.

Expected Completion Date: Completed. Completion date: November 16, 2023.

VA requests closure of Recommendation 3.

Recommendation 4: Ensure network segmentation controls are applied to all network segments with special-purpose systems.

Comments: Non-concur.

VA non-concurs with OIG’s recommendation. VA is following VA policies concerning network segmentations.

Expected Completion Date: Completed. Completion date: not applicable.

VA requests closure or removal of Recommendation 4.

Recommendation 5: Implement a process to retain database logs for a period consistent with VA’s record retention policy.

Comments: Concur.

The Infrastructure Operations, Platforms Support, and Database Management Service Line implemented processes to retain database logs.

Expected Completion Date: Completed. Completion date: May 20, 2024.

VA requests closure of Recommendation 5.

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 Keith Hargrove Timothy Moorehead Kimberly Moss Albert Schmidt Justin Skeen Brandon Zahn
Other Contributors	Allison Tarmann Rashiya Washington

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, Southwest Consolidated Mail Order Pharmacy

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
US Senate: Mark Kelly, Kyrsten Sinema
US House of Representatives: Juan Ciscomani, Raúl M. Grijalva

OIG reports are available at www.vaoig.gov.