DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS HEALTH ADMINISTRATION

Inspection of Information Technology Security at the Consolidated Mail Outpatient Pharmacy in Tucson, Arizona

INFORMATION TECHNOLOGY INSPECTION

REPORT #21-02453-99

JUNE 1, 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.

FOR MORE
VA OIG REPORTS
CLICK HERE

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 (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.[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 (FY) 2020 FISMA audit made 26 recommendations to VA. Repeat recommendations included addressing deficiencies in configuration management, contingency planning, security management, and access controls.[3] Appendix A details these recommendations. The report concluded that VA continues to face significant challenges in meeting FISMA requirements.

In 2020, the OIG started an IT security inspection program. These IT inspections assess whether VA facilities are meeting federal security requirements related to configuration management, contingency planning, security management, and access controls.[4] They are typically conducted at selected facilities that have not been assessed under the annual audit required by FISMA or at facilities that previously performed poorly on the annual FISMA audit.

The OIG conducted this inspection to determine whether the Tucson Consolidated Mail Outpatient Pharmacy (CMOP) in Arizona was meeting federal security guidance. The inspection team selected the Tucson CMOP because it is home to the CMOP Local Area Network, which establishes an interface for the electronic transfer of information between all Veterans Health Administration medical centers and the CMOP host systems located at each of the seven CMOPs. These CMOPs form an integrated and highly automated outpatient prescription dispensing system. The inspection scope and methodology are described in appendix C.

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

[2] Joint Task Force, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, rev. 5, National Institute of Standards and Technology (NIST), 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.

What the Inspection Found

The OIG IT inspections are focused on four security control areas that apply to local facilities. These control areas have been selected based on their levels of risk; without these controls, VA's systems are at risk of unauthorized access or modification:

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] Contingency planning also 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, such as authorization, visitors, monitoring, delivery, and removal.[8]

The Tucson CMOP Had Deficiencies in Configuration Management Controls

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

- **Component inventory** is a descriptive record of IT assets in an organization down to the system level.
- **Vulnerability management** is the process by which the Office of Information and Technology (OIT) identifies, classifies, and reduces weaknesses.

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

[6] GAO, *FISCAM*.

[7] GAO, *FISCAM*.

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

- **Flaw remediation** is how organizations correct software defects and often includes system updates, such as security patches.[9]
- **Configuration management plans** identify configuration management roles and responsibilities, resources, and processes to ensure any changes are evaluated and approved before implementation.

The Tucson CMOP did not have accurate inventories, which led to other security management control deficiencies. A complete, accurate, and up-to-date inventory is required to implement an effective security program.[10] Inaccurate component inventories affect vulnerability and patch management effectiveness.

The inspection team determined that OIT's standard vulnerability identification process and scans were ineffective. OIT scans for vulnerabilities routinely, randomly, and 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 found on multiple computers. The inspection team identified 124 vulnerabilities—24 critical vulnerabilities on 141 computers and 100 high-risk vulnerabilities on 164 computers—which were not mitigated within the time frames established by OIT. The team also found 10 critical vulnerabilities and 16 high-risk vulnerabilities that OIT did not detect.

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.

The inspection team found that the configuration management plan was developed as required by the standard operating procedures and that it had been disseminated for review. However, the configuration management plan had not been fully implemented. The CMOP roles and responsibilities identified within the approved CMOP configuration plan were not implemented. For example, the CMOP Change Implementation Board was not developed, which primarily resulted in lack of documentation for life-cycle configuration management activities and lack of central management, including audit reports, status reports, metrics, and change history documentation.

[9] NIST Special Publication 800-53.

[10] GAO, *FISCAM.*

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

The Tucson CMOP Had Deficiencies in Contingency Planning Controls

Contingency planning controls provide reasonable assurance that resources are protected, minimize the risk of unplanned interruptions, and provide for recovery of critical operations should interruptions occur. The Tucson CMOP had security deficiencies in contingency plans, which contain detailed guidance and procedures for restoring damaged systems unique to the systems' security impact level and recovery requirements.

The Tucson CMOP has not developed or put into place disaster recovery plans as required by VA authorization procedures. Without disaster recovery plans, the Tucson CMOP risks service interruption and a backlog of prescriptions to be filled by other CMOPs. The impact to operations would be prolonged because resources for databases would need to be recreated to restore operations.

No Deficiencies Were Identified for Security Management Controls at the Tucson CMOP

During its inspection of the Tucson CMOP, the inspection team did not identify significant deficiencies in the controls implemented for security management other than a minor delay in updating policies that were inherited from a deactivated enclave.[12]

The Tucson CMOP Had Deficiencies in Access Controls

According to the FISCAM, access controls provide reasonable assurance that access to computer resources (data, equipment, and facilities) is restricted to authorized individuals. The Tucson CMOP had security deficiencies in the following access controls:

- **Account management** is the process of requesting, establishing, issuing, and closing user accounts; tracking users and their respective access authorizations; and managing these functions.
- **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, to recognize an attack, and to investigate during or after an attack.[13]

The inspection team found that the Tucson CMOP did not change the default login and password for their security camera system, which is an account management weakness for this system. The

[12] An enclave is a set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter.

[13] GAO, *FISCAM*.

team was able to access facility security cameras, including features that allowed control of the camera's zoom and panning abilities. An attacker with knowledge of the default password and network access to the security camera system could log in and take control of the system and use it to facilitate identity theft, to identify physical security weakness, and to deny access to the system. Further, the camera system was used as a compensating control to deter and identify theft by employees or identify access for systems that lacked authentication measures. Since the camera system is a compensating control—meaning it is in place due to a lack of a different recommended control—it is critically important to adequately protect access to the system.

The inspection team also identified weaknesses in Tucson CMOP's audit and monitoring controls after they reviewed a sample of audit logs from a 24-hour period in the OIT audit log systems. The analysis indicated that 290 of 624 Tucson CMOP systems failed to generate or forward audit logs to the Cybersecurity Operations Center for analysis as required by local policy. Without audit records, VA cannot identify, review, analyze, and report inappropriate or suspicious activity occurring on the Tucson CMOP network.

What the OIG Recommended

The OIG made the following recommendations to the Tucson CMOP director:

1. Implement more effective inventory management tools for all network segments.
2. Implement a more effective vulnerability and flaw remediation program that can accurately identify vulnerabilities and enforce flaw remediation.
3. Develop and implement methods to ensure delivery, receipt, and understanding of assigned roles and responsibilities for Consolidated Mail Outpatient Pharmacy activities to ensure full implementation of approved policy.
4. Develop and implement a disaster recovery plan and capability that will restore operations in the event of a disruption to critical operations.
5. Task the facility manager to change the default username and password for the security camera system.
6. Request the Office of Information and Technology to configure audit logging on the misconfigured devices in accordance with established baselines, policy, and procedures.

VA Comments and OIG Response

The assistant secretary for information and technology and chief information officer provided comments for the Tucson CMOP (appendix D). OIT concurred with recommendations 1, 3, 4, 5, and 6 and requested recommendations 1, 3, 5, and 6 be closed due to corrective actions it reported were completed.

OIT did not concur with recommendation 2 to implement a more effective vulnerability and flaw remediation program that can accurately identify vulnerabilities and enforce flaw remediation. The assistant secretary reported that within the time frame of the inspection, OIT was able to demonstrate vulnerability identification, remediation, mitigation, and management rates of 92 percent for all critical and high-risk vulnerabilities at the Tucson CMOP. The assistant secretary also stated that VA consistently maintains a 90 percent or greater vulnerability management rate for all critical and high-risk vulnerabilities across the enterprise. OIT believes this demonstrates that it has implemented and is managing an effective vulnerability and flaw remediation program aligned with federal and industry standards.

Regarding the nonconcurrence with recommendation 2, OIT did not provide evidence that would allow the OIG to validate the assertion that it demonstrated vulnerability identification, remediation, mitigation, and management rates of 92 percent for all critical and high-risk vulnerabilities. The OIG identified 22 critical vulnerabilities within its vulnerability scans, while OIT scans identified 12, which is 45 percent less than the OIG. The OIG also identified 100 high-risk vulnerabilities, while OIT scans identified 84, which is 16 percent less than the OIG. Accordingly, the OIG disagrees with management's assertion that VA's vulnerability management program is effective. The OIG's conclusion is based on known vulnerabilities that were not identified by OIT or mitigated within time frames established by OIT. Therefore, the OIG stands by its recommendation 2 and that recommendation remains open. The full text of the response from the assistant secretary is included in appendix D.

OIT provided responsive actions plans for the five recommendations with which it concurred. Based on evidence provided, the OIG considers recommendations 1, 3, and 5 closed. The OIG will monitor implementation of planned actions and close the remaining open recommendations when VA provides sufficient evidence demonstrating progress in addressing the recommendations and the issues identified.

Larry M. Reinkemeyer

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluation

Contents

Executive Summary i

Abbreviations viii

Introduction 1

Results and Recommendations 6

Finding 1: The Tucson CMOP Had Deficiencies in Configuration Management Controls 8

Recommendations 1–3 12

Finding 2: The Tucson CMOP Did Not Have Disaster Recovery Plans in Contingency Planning Controls 15

Recommendation 4 16

Finding 3: No Weaknesses Were Found in Security Management Controls 18

Finding 4: The Tucson CMOP Had Deficiencies in Account Management and Audit and Monitoring Controls 19

Recommendations 5–6 21

Appendix A: FISMA Audit for FY 2020 Report Recommendations 23

Appendix B: Background 26

Appendix C: Scope and Methodology 28

Appendix D: VA Management Comments 30

OIG Contact and Staff Acknowledgments 33

Report Distribution 34

Abbreviations

CMOP	Consolidated Mail Outpatient Pharmacy
CSOC	Cyber Security Operations Center
DevSecOps	Office of Development, Security, and Operations
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Modernization Act
FY	fiscal year
GAO	Government Accountability Office
IT	information technology
ITOPS	Information Technology Operations and Services
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 Tucson Consolidated Mail Outpatient Pharmacy (CMOP) in Arizona was meeting federal security requirements and complying with related guidance.[14] The inspection team selected the Tucson CMOP because it is home to the CMOP Local Area Network, which establishes an interface for the electronic transfer of information between all Veterans Health Administration medical centers and the CMOP host systems located at each of the seven CMOPs. These CMOPs form an integrated and highly automated outpatient prescription dispensing system.

The Federal Information Security Modernization Act (FISMA) of 2014 was established, in part, to improve oversight of federal agency information security programs.[15] In accordance with the act, VA must develop, document, and implement an agencywide information security and risk management 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. 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.[16] The OIG IT inspection program reviews sites not evaluated under the annual FISMA audits—only a sample of facilities are examined during the FISMA audits—or at those facilities that did not perform well in prior FISMA audits. The OIG's IT inspections are not intended to replicate 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 OIG 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):

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

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

[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 law, including FISMA and its implementing regulations, requires federal agencies to protect sensitive data and information systems due to the risk of harm that could result from improper disclosure. Accordingly, the memorandum is not being published by the OIG or distributed outside of VA to prevent intentional or inadvertent disclosure of specific vulnerabilities or other information that could be exploited to interfere with VA's network operations and adversely affect the agency's ability to accomplish its mission.

Table 1. Security Controls Evaluated in this Report

Security control area	Definition	Examples 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 modification. A cyberattack could disrupt, destroy, or allow 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.[17]

According to VA Handbook 6500, the responsibility for developing and maintaining information security policies, procedures, and control techniques lies with the assistant secretary for information and technology, who is also VA's chief information officer. VA Handbook 6500 describes the risk-based process for selecting system security controls, including operational

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

requirements.[18] 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 (also the 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 and acts as a steward for VA's IT assets and resources." There are four groups in OIT that touch on the issues addressed in this report. The Cybersecurity Operations Center (CSOC) is part of OIT's Office of Information Security. CSOC 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 (DevSecOps) unifies software development, software operations, service management, information assurance, cybersecurity compliance, performance monitoring, and technical integration throughout the entire solution delivery process (figure 1).

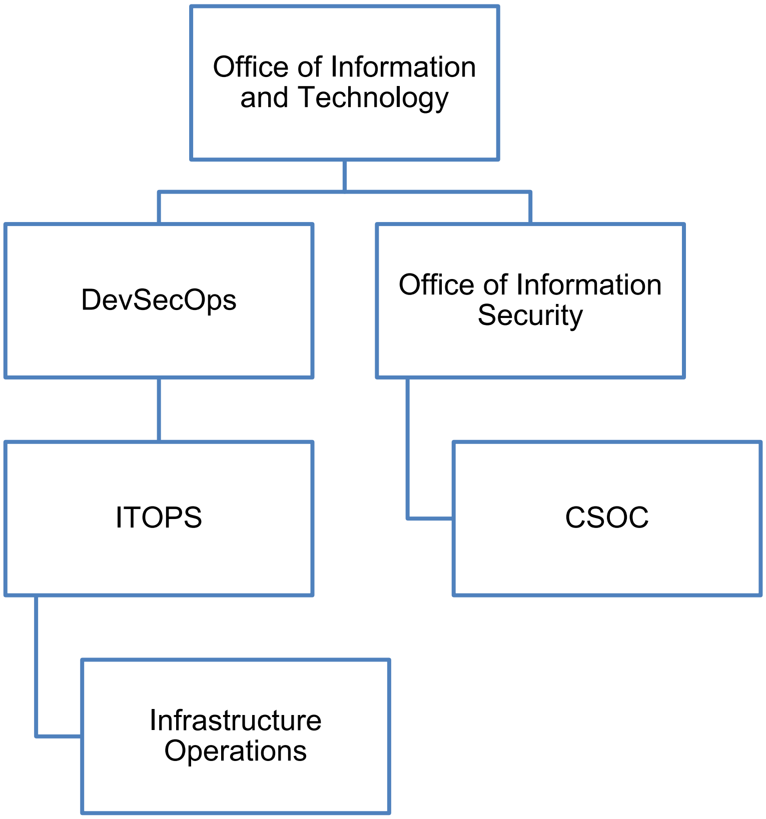
Office of Information and Technology
DevSecOps
Office of Information Security
ITOPS
CSOC
Infrastructure Operations

Figure 1. *Organizational structure of entities relevant to this inspection.*

Source: VA OIG analysis.

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

OIT's Information Technology Operations and Services (ITOPS) provides standardized customer service, technology implementation, and technical support. According to their mission statement, Infrastructure Operations strives to be a customer-centric organization focused on efficiently delivering secure and high-availability infrastructure solutions in support of VA's mission. OIT assigns dedicated Infrastructure Operations personnel to the Tucson CMOP.

Fiscal Year (FY) 2020 FISMA Audit

The OIG issues annual reports on VA's information security program based on audits conducted by CliftonLarsonAllen LLP, an independent public accounting firm. The FY 2020 FISMA audit evaluated 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.[19] CliftonLarsonAllen LLP made 26 recommendations, listed in appendix A. Of these recommendations, 23 are repeated from the prior annual audit, indicating that VA continues to face significant challenges in complying with FISMA requirements.[20]

Related Government Accountability Office Review

A November 2019 Government Accountability Office (GAO) review found that VA continued to have a deficient information security program.[21] According to the GAO, as VA secured and modernized its information systems, VA faced several security challenges, 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.

[19] 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 that share common functionality.

[20] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2019,* Report No. 19-06935-96, March 31, 2020. Appendix B presents information about FISMA and other federal criteria and standards discussed in this report.

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

The GAO concluded that "until VA adequately mitigates security control deficiencies, the sensitive data maintained on its systems will remain at risk of disruption and have an increased risk of unauthorized modification and disclosure."[22]

Tucson CMOP

The Pharmacy Benefits Management Services operate the VA CMOPs, including the Tucson CMOP (shown in figure 2). Combined, the VA CMOPs processed 125 million prescriptions in FY 2019. Approximately 80 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 Medical Program.

The Tucson CMOP facility is approximately 80,000 square feet and is located on 4.55 acres. The Tucson CMOP's annual budget is almost $958 million, and it processed almost 24 million prescriptions in FY 2020. VA medical sites in Alaska, Arizona, California, Colorado, Hawaii, Idaho, Oregon, New Mexico, Nevada, Utah, Washington, and Wyoming are assigned to the Tucson CMOP.

Figure 2. *Tucson CMOP.*

Source: Vulnerability Assessment Southwest Consolidated Mail Outpatient Pharmacy; Southern Arizona VA Health Care System, Chief of Police.

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

Results and Recommendations

The inspection team reviewed configuration management, contingency planning, security management, and access controls at the Tucson CMOP. Within configuration management, the team identified deficiencies with component inventory, vulnerability management, flaw remediation, and implementation of the configuration management plan.

The inspection team's review of contingency planning controls showed that VA's policies and procedures addressed control criteria such as identifying critical operations, implementing environmental controls, and performing preventative maintenance. However, VA did not develop or put into place disaster recovery plans.

During the evaluation of security management controls, the team did not identify deficiencies associated with the security program, assessment and validation of risk, control implementation, awareness and personnel security, monitoring, remediation, or third-party security.

Finally, the inspection team reviewed access controls, including boundary protection, sensitive resources, physical security, system audit, identification, authentication, and authorization. The team identified deficiencies in account management and audit and monitoring controls.

Configuration Management Controls

According to the GAO's *Federal Information System Controls Audit Manual* (FISCAM), configuration management involves identifying and managing security features for all hardware, software, and firmware components of an information system at a given point and systematically controlling changes to that configuration during the system's life cycle.[23] The inspection team reviewed and evaluated the 23 configuration management controls for VA-hosted systems (drawn from NIST criteria) at the Tucson CMOP to determine if they met federal guidance and VA requirements. The 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

[23] GAO, *FISCAM*.

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.[24] 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 the use of noncurrent software. Examples of these controls are software usage restrictions, user-installed software, malicious code protection, security alerts, and advisories. Examples of controls in this element are vulnerability scanning, flaw remediation, malicious code protection, security alerts, and advisories.
- **Document and have emergency changes approved** by appropriate entity officials and notify appropriate personnel for follow-up and analysis of the changes. It is not uncommon for program changes to be needed on an emergency basis to keep a system operating. However, due to the increased risk of errors, emergency changes should be kept to a minimum.

An effective configuration management process consists of four primary concepts (identification, control, status accounting, and auditing), each of which should be described in a configuration management plan and implemented according to the plan. VA must first establish an accurate component inventory to identify all computers on the network. Component inventories affect the success of other controls, such as vulnerability and patch management. OIT's CSOC identifies and reports threats and vulnerabilities for VA. Once this process is complete, OIT's Patch and Vulnerability Team develops procedures to remediate identified issues, which may include applying patches. This process helps secure computers from attack.

[24] 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 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.[25]

Finding 1: The Tucson CMOP Had Deficiencies in Configuration Management Controls

To assess configuration management controls, the inspection team interviewed the systems owner, information system security officers, system stewards, and personnel from the CMOP Systems Program Management Office. The team observed the system change management processes; reviewed local policies, procedures, and inventory lists; and scanned the Tucson CMOP's network to identify devices. The team compared the devices found on the network with the OIT inventories of the two systems; it also received vulnerability lists provided by OIT and scanned the Tucson CMOP's network to identify vulnerabilities.[26] Both comparisons of the devices and the vulnerability scans showed that OIT did not

- have an accurate component inventory list;
- identify all critical or high-risk vulnerabilities in the network; and
- remediate flaws including unsupported versions of applications, missing patches, and vulnerable plug-ins.

By not implementing more effective configuration management controls, VA is placing critical systems at unnecessary risk of unauthorized access, alteration, or destruction. Additionally, the inspection team found that the CMOP configuration management plan was not fully implemented. For example, the Change Implementation Board was not developed, and the responsibilities of key stakeholders were not fulfilled as identified in the plan. 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.

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

[25] The Tucson CMOP hosted two systems (the Tucson CMOP network and CMOP Pharmaceutical System, which supports all seven CMOPs) authorized to operate on the VA network; however, many of the two-system configuration management controls were inherited from VA's general support systems, which are assessed in the annual FISMA audits and thus were not evaluated by the inspection team.

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

effective information security program because it provides greater visibility into and control over these systems.[27] 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 Tucson CMOP, despite OIT and VA's use of automated systems to maintain a readily available baseline of its information systems. VA identified 330 devices in the CMOP's inventory. However, the team identified 624 devices. This review also revealed devices in multiple accreditation boundaries and virtual local area networks not associated with Tucson CMOP network and CMOP Pharmaceutical System.[28]

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 Tucson CMOP. According to the 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."[29] 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. CSOC identifies and reports threats and vulnerabilities for VA, and OIT conducts scans for vulnerabilities routinely, randomly, or when new vulnerabilities are identified and reported.[30]

However, OIT'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. Unsupported applications do not receive 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 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.[31] The

[27] GAO, *FISCAM*.

[28] An accreditation boundary is all components of an information system to be accredited by an authorizing official and excludes separately accredited systems to which the information system is connected. A virtual local area network is the logical partitioning of devices connected to a physical network that can be configured as if they were connected to their own physical local area network.

[29] 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."

[30] VA Handbook 6500.

[31] "Vulnerability Metrics," NIST, accessed August 21, 2020, 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 (FIRST), accessed March 13, 2020, https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf.

scoring system captures the principal characteristics of a vulnerability and produces a numerical score reflecting its severity. Numerical scores are classified as risk levels (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, whereas high-risk vulnerabilities have a score between 7.0 and 8.9. OIT establishes time frames for remediating vulnerabilities based on their severity.

The inspection team compared OIT-provided network vulnerability scan results from the Tucson CMOP against scans conducted by the OIG team from June 14 to June 18, 2021. The team and OIT used the same vulnerability scanning tools. The team identified 124 vulnerabilities (24 critical vulnerabilities on 141 computers and 100 high-risk vulnerabilities on 164 computers), which were not mitigated within the time frames established by OIT. 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. The team determined that OIT's scans were inadequate because the team found 10 critical vulnerabilities and 16 high-risk vulnerabilities that OIT did not detect.

Unidentified threats cannot be mitigated; they represent weaknesses that could be exploited to gain access to VA data. Organizations, therefore, should periodically perform assessments to protect information, address vulnerabilities, and make decisions about accepting or mitigating risks.[32]

Flaw Remediation

The Tucson CMOP 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 and no new security patches will be created. Devices missing patches contain known vulnerabilities that the patches are intended to correct. Attackers can exploit these vulnerabilities and vulnerable plug-ins in web browsers.[33]

[32] NIST, *Managing Information Risk*, NIST Special Publication 800-39, National Institute of Standards and Technology (NIST), 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."

[33] NIST, *Security Guide for Interconnecting Information Technology Systems*, NIST Special Publication 800-47, National Institute of Standards and Technology (NIST), 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."

Flaw remediation is the process by which organizations correct software defects, including applying updates such as patches.[34] Patches are usually the most effective way to mitigate software flaw vulnerabilities and are often the only fully effective solution. According to the 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.[35]

VA's CSOC conducts periodic independent scans of all VA-owned systems. The discovered vulnerabilities are entered into a plan of action and milestones for remediation by the system owners. The information system owner/system steward utilizes the Remediation Effort Entry Form to document mitigation/remediation efforts for each deficiency identified from the scan and provides evidence that the deficiencies have been mitigated.

Despite VA's significant patch management measures, the inspection team identified several devices that were missing patches. For example, several database servers were missing security patches for critical and high-risk vulnerabilities. Databases often contain mission-critical data or sensitive data, which makes them obvious targets for exploitation. 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.

Configuration Management Plan

The configuration management plan identifies configuration management roles and responsibilities, resources, and processes to ensure any changes are evaluated and approved before implementation. Further, these policies and procedures should be developed, documented, and implemented at the entity-wide, system, and application levels to ensure an effective configuration management process. The Office of Information Security Authorization Requirements Standard Operating Procedures were developed to ensure systems obtain and maintain a VA Authorization to Operate.[36] These procedures provide guidance to information

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

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

[36] Office of Information Security, "Authorization Requirements," Standard Operating Procedure, version 1.24, May 13, 2021.

system security officers, system owners, and system stewards on the steps to obtain an authorization to operate and templates for products such as the configuration management plan.

The inspection team found that the configuration management plan was developed and approved as required by the standard operating procedure and that the plan had been disseminated for review. However, the plan had not been fully implemented. Specifically, the CMOP roles and responsibilities identified were not being carried out according to the plan. For instance, the CMOP Change Implementation Board did not function as planned, which resulted in a lack of life cycle configuration management activity and documentation such as audit reports, status reporting, metrics, and change history documentation.

Finding 1 Conclusion

The Tucson CMOP did not have accurate inventories, which led to undetected and unaddressed critical and high-risk vulnerabilities within its systems. Additionally, the CMOP configuration management plan was not fully implemented, which prevented key stakeholders from providing expected capabilities and functions. Effective configuration management prevents unauthorized changes to information system resources (e.g., software programs and hardware configurations) and provides reasonable assurance that systems are configured and operating securely and as intended. The absence of effective system-level configuration management is a serious risk that jeopardizes an entity’s ability to support current and potential requirements. Without effective configuration management, users do not have adequate assurance that the system and network will perform as intended and to the extent needed to support their missions.

Recommendations 1–3

The OIG made the following recommendations to the director of the Tucson CMOP:

1. Implement more effective inventory management tools for all network segments.
2. Implement a more effective vulnerability and flaw remediation program that can accurately identify vulnerabilities and enforce flaw remediation.
3. Develop and implement methods to ensure delivery, receipt, and understanding of assigned roles and responsibilities for Consolidated Mail Outpatient Pharmacy activities to ensure full implementation of approved policy.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 1 and 3. The assistant secretary reported OIT has implemented physical and logical inventory changes that resulted in the CMOP complying with inventory requirements. The assistant secretary also reported that the CMOP has updated the configuration management plan and updated the CMOP accreditation boundary to include infrastructure and storage devices, which facilitates scanning and vulnerability remediation based on internet protocol range and helps prevent duplicate accounting of assets in the electronic Enterprise Mission Assurance Support Service inventory.

The assistant secretary did not concur with recommendation 2. The assistant secretary reported that within the time frame of the inspection, OIT was able to demonstrate vulnerability identification, remediation, mitigation, and management rates of 92 percent for all critical and high-risk vulnerabilities at the Tucson CMOP. The assistant secretary also stated that VA consistently maintains a 90 percent or greater vulnerability management rate for all critical and high-risk vulnerabilities across the enterprise. OIT believes this demonstrates that it has implemented and is managing an effective vulnerability and flaw remediation program aligned with federal and industry standards.

OIG Response

The assistant secretary reported the corrective actions regarding recommendation 1 and 3 were completed, and OIT provided sufficient evidence to support that the actions were completed. As a result, the OIG considers recommendations 1 and 3 closed.

Regarding the nonconcurrence with recommendation 2, OIT did not provide evidence that would allow the OIG to validate the assertion that OIT demonstrated vulnerability identification, remediation, mitigation, and management rates of 92 percent for all critical and high vulnerabilities. The OIG identified 22 critical vulnerabilities within its vulnerability scans, while OIT scans identified 12, which is 45 percent less than the OIG. The OIG also identified 100 high vulnerabilities, while OIT scans identified 84, which is 16 percent less than the OIG. Accordingly, the OIG disagrees with management’s assertion that VA’s vulnerability management program is effective.

The OIG’s conclusion is based on known vulnerabilities that were not mitigated within policy time frames established by OIT. Therefore, the OIG stands by its recommendation 2. 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 the 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

- assessing the criticality and sensitivity of computerized operations and identification of supporting resources,
- taking steps to prevent and minimize potential damage and interruption,
- establishing a comprehensive contingency plan, and
- periodically testing the contingency plan with appropriate adjustments based on testing.[37]

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, the plans 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."[38] 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 (e.g., temporary power failures) as well as disasters such as fires, natural disasters, and acts of terrorism that would require reestablishing operations at a remote location.

To determine if the Tucson CMOP met federal guidance and VA requirements, the inspection team evaluated 22 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.

[37] GAO, *FISCAM*.

[38] FISMA of 2014.

- **Contingency training and testing** validate recovery capabilities and prepare recovery personnel for plan activation.
- **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 occurs after 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 and include activities such as maintaining fire suppression systems, smoke or water detectors, redundant cooling systems, and backup power supplies.

Finding 2: The Tucson CMOP Did Not Have Disaster Recovery Plans in Contingency Planning Controls

To assess contingency planning controls, the inspection team interviewed the systems owner, information system security officers, system stewards, and personnel from the CMOP Systems Program Management Office. The team also reviewed local policies and procedures.

The inspection team found that VA's policies and procedures addressed control criteria such as identifying critical operations, implementing environmental controls, and performing preventative maintenance. However, the Tucson CMOP did not have disaster recovery plans in the event of a catastrophic failure and loss of its networking environment. The system steward acknowledged that they were working toward a disaster recovery capability. By not developing and putting in place disaster recovery plans, VA is risking interruption of operations at the Tucson CMOP, which would cause a prescription backlog that would be distributed to other CMOPs until operations could be restored. Further, the lack of a disaster recovery plan would prolong recovery efforts because resources would need to be recreated to restore critical databases. Additionally, when assessing authorization requirements for the CMOP, the information system owners did not properly address the need for disaster recovery operations.

VA requires system owners or system stewards to work with information system security officers to create disaster recovery plans.[39]

Finding 2 Conclusion

The Tucson CMOP has not developed disaster recovery plans or put them into policy as required by VA authorization procedures. Without disaster recovery plans, Tucson CMOP operations are at risk of interruption, which could result in a backlog of prescriptions that would need to be filled by other CMOPs. The impact to operations would potentially be prolonged because resources for databases would need to be recreated to restore operations.

Recommendation 4

The OIG made the following recommendation to the director of the Tucson CMOP:

4. Develop and implement a disaster recovery plan and capability that will restore operations in the event of a disruption to critical operations.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with the recommendation and stated the Tucson CMOP has a disaster recovery plan, but it does not meet the recovery time objective. The assistant secretary stated that the facility is building the disaster recovery plan site to meet this requirement with an estimated completion date of June 30, 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.

[39] Office of Information Security, "Authorization Requirements."

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 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 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 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 are 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 reassessing related risks, applying appropriate corrective actions, and follow-up monitoring to ensure actions are effective. Agencies develop plans of actions and milestones to track weaknesses and corresponding corrective actions.

- **Ensure third parties are secure,** as vendors, business partners, and contractors are often granted access to systems for purposes such as outsourced software development or system transactions.[40]

Finding 3: No Weaknesses Were Found in Security Management Controls

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 interviewed information system security officers, local administrators, contracting officer's representatives, human resources staff, privacy officers, and system stewards.

The Tucson CMOP security management program has a comprehensive risk assessment process; local policies contained the required information, and the CMOP has appropriate policies and procedures to monitor the activities of external third parties. The team did identify policies that were inherited from a deactivated enclave that need to be updated but still contained the required information.[41] The team did not identify any deficiencies in the Tucson CMOP's security management controls other than the lapse in updating policies. Accordingly, the OIG did not make any recommendations for improvement.

[40] GAO, *FISCAM*.

[41] An enclave is a set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter.

Access Controls

Previous FISMA reports have repeatedly identified access controls as a nationwide issue for VA. Access controls, including boundary protections, sensitive system resources, physical security, and audit and monitoring controls 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 Tucson CMOP, the inspection team reviewed all six critical access control 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; environmental controls such as smoke detectors, fire alarms, and extinguishers; and uninterruptible power supplies.
- **Audit and monitoring controls** involve the collection, review, and analysis of events for indications of inappropriate or unusual activity. These controls should be routinely used to assess the effectiveness of other security controls, to recognize an attack, and to investigate during or after an attack.
- **Identification and authentication controls** distinguish one user from another and establish the validity of a user's claimed identity.
- **Authorization controls** determine what users can do, such as granting access to various resources, and depend on valid identification and authentication controls. These controls establish the validity of a user's claimed identity.

Finding 4: The Tucson CMOP Had Deficiencies in Account Management and Audit and Monitoring Controls

To evaluate Tucson CMOP'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 a walk-through of the facility; and analyzed audit logs.[42]

The team determined that

- account management had weaknesses because the Tucson CMOP did not change the default login and password for their security camera system, and
- auditing and monitoring controls had weaknesses because systems at the Tucson CMOP failed to generate and forward audit reports to CSOC for analysis.

Account Management

The inspection team identified weaknesses in the Tucson CMOP's account management for its security camera system. Account management is the process of requesting, establishing, issuing, and closing user accounts; tracking users and their respective access authorizations; and managing these functions.[43] The CMOP did not change the default login and password for its security camera system. The team was able to access facility security cameras, including features that allowed control of the camera's zoom and panning abilities. The system was not checked after installation to eliminate this vulnerability. Developers may deliver system components with factory default authentication credentials (i.e., passwords) for initial installation and configuration. An attacker with knowledge of the default password and network access to a system can log in and take control of the system and use it to facilitate identity theft, to identify physical security weakness, or to deny access to the system. Further, per an interview with the facility manager, the camera system was used as a compensating control to deter and identify theft by employees or identify access for systems that lacked authentication measures. Compensating controls are employed in lieu of a recommended control, which provides equivalent or comparable protection. Since the camera system is a compensating control for other controls, it is critically important to adequately protect access to the system.

Audit and Monitoring

The inspection team identified weaknesses in the Tucson CMOP's audit and monitoring controls. The team reviewed policies and procedures, interviewed appropriate personnel, and reviewed a sample of audit logs over a 24-hour period from OIT's audit log systems. The Tucson CMOP's existing policies and procedures addressed auditable events and responsible parties. However, analysis of log data received from CSOC indicated that 290 of 624 Tucson CMOP systems failed to generate or forward audit logs to CSOC for analysis as required by local policy.[44]

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

[43] GAO, *FISCAM*.

[44] Infrastructure Operations Cybersecurity Management, "Audit Log Analysis and Retention," Standard Operating Procedure, March 7, 2019.

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 Tucson CMOP network.

Finding 4 Conclusion

The Tucson CMOP did not change the default login and password for its security camera system, which increases the risk of identity theft, physical security weakness, and denial of service to veterans. Also, the Tucson CMOP is not generating and forwarding audit reports for many of its systems, minimizing VA's ability to review, analyze, and report inappropriate or suspicious activity in the network.

Recommendations 5–6

The OIG made the following recommendations to the director of the Tucson CMOP:

5. Task the facility manager to change the default username and password for the security camera system.
6. Request the Office of Information and Technology to configure audit logging on the misconfigured devices in accordance with established baselines, policy, and procedures.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 5 and 6. The assistant secretary reported that default usernames and passwords for the security camera systems have been updated to meet security requirements. The assistant secretary also stated that manual checks were performed to confirm logging was in place for the servers in question. Some of the systems were no longer live, some were clusters consolidated back to the original active hosts, and the remaining active hosts were confirmed to be logging.

OIG Response

The corrective actions reported by the assistant secretary are responsive to the intent of the recommendations. Based on evidence provided, the OIG considers recommendation 5 closed. The OIG will monitor implementation of the actions in response to recommendation 6 and will close the recommendation when VA provides sufficient evidence demonstrating progress in addressing the issues identified.

Overall Conclusion

The inspection team identified deficiencies in component inventory, vulnerability management, flaw remediation, configuration management planning, disaster recovery planning, account management, and monitoring of audit logs. The OIG made six recommendations to the director of the Tucson CMOP: (1) Implement more effective inventory management tools for all network segments; (2) Implement a more effective vulnerability and flaw remediation program that can accurately identify vulnerabilities and enforce flaw remediation; (3) 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; (4) Develop and implement a disaster recovery plan and capability that will restore operations in the event of a disruption to critical operations; (5) Change the default username and password for the security camera system; and (6) Configure audit logging on the misconfigured devices in accordance with established baselines, policy, and procedures.

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

Appendix A: FISMA Audit for FY 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 Tucson CMOP. The 26 recommendations are listed below:

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, risk assessments, 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 a specific methodology for evaluating the confidentiality, integrity, and availability of information systems. FISCAM groups related controls into categories that have similar risks. To assist auditors in evaluating information systems, FISCAM maps control categories to NIST controls.

Federal Information Security Modernization Act of 2014

The stated goals of FISMA are as follows:

- 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.[45]

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.

[45] FISMA of 2014.

NIST Information Security Guidelines

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

Appendix C: Scope and Methodology

Scope

The inspection team conducted its work from May 2021 through January 2022. When the team inspected the Tucson CMOP during the week of June 14, 2021, the facility was normally staffed as the nature of the work requires employees to be on-site. Due to COVID-19 restrictions, the team maintained social distance from the Tucson CMOP staff and followed the Centers for Disease Control and Prevention's recommendations, including wearing masks. To further limit contact with CMOP personnel, most interview attendees participated 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 interviewed VA personnel responsible for CMOP 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.[46]

The team used the GAO's FISCAM as a template to plan for inspections. When planning for this review, the team identified potential information system controls that would significantly impact the review. Specifically, the team used FISCAM's appendix II as a guide to help develop evidence requests and a base set of interview questions for the Tucson CMOP and its personnel.

[46] VA Handbook 6500.

The team also used the FISCAM controls identified in appendix II as an overlay to correlate FISMA controls used by VA to protect and secure their 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 assessed in both assessments due to redundant roles and responsibilities among VA's local, regional, and national facilities and offices.

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

Fraud Assessment

The inspection team assessed the risk that fraud and noncompliance with provisions of laws, regulations, contracts, and grant agreements, significant within the context of the inspection 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 and then compared it to the expected version. If the system did not have the current software version, the tool identified that as a vulnerability. As the security tools did not alter data, the team determined that the output was reliable. The data were complete and accurate, met intended purposes, and were not subject to alteration.

Government Standards

The OIG conducted this 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: March 23, 2022

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

Subj: OIG Draft Report: Inspection of Information Technology Security at the Consolidated Mail Outpatient Pharmacy in Tucson, Arizona, Project Number 2021-02453-AE-0110 (VIEWS V06847732)

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

1. The Office of Information and Technology (OIT) is responding to the Office of Inspector General (OIG) Draft Report, Inspection of Information Technology Security at the VA Tucson Consolidated Mail Outpatient Pharmacy (CMOP).

2. In 2020, the OIG started an information technology (IT) security inspection program. The IT inspections help identify whether VA facilities are meeting federal security requirements related to configuration management, contingency planning, security management and access controls. They are typically conducted at selected facilities that have not been assessed under the annual audit required by the Federal Information Security Modernization Act (each audit focuses on a sample) or at facilities that previously performed poorly on the annual audit. The OIG conducted this inspection to determine whether the Tucson Consolidated Mail Outpatient Pharmacy (CMOP) was meeting federal security guidance. The inspection team selected the Tucson CMOP because it is home to the CMOP Local Area Network, which establishes an interface for the electronic transfer of information between all Veterans Health Administration Medical Centers and the CMOP host systems located at each of the seven CMOPs. These CMOPs form an integrated and highly automated outpatient prescription dispensing system.

3. The OIG IT inspection found the Tucson CMOP had deficiencies in Configuration Management Controls, Contingency Management Planning Controls and Access Controls. There were no deficiencies identified for Security Controls at the Tucson CMOP. The OIG made six recommendations to the Tucson CMOP Director.

4. OIT submits written comments, supporting documentation and a target completion date for each recommendation.

The OIG removed point of contact information prior to publication.

(Original signed by)

Kurt D. DelBene

Attachment

005 Attachment

Office of Information and Technology

Comments on OIG Draft Report,

Inspection of Information Technology Security at the Consolidated Mail Outpatient Pharmacy in Tucson, Arizona, Project Number 2021-02453-AE-0110(VIEWS 06847732)

Recommendation 1: The OIG recommends the Tucson CMOP director implement more effective inventory management tools for all network segments.

Comments: Concur. The Department of Veterans Affairs (VA) Office of Information and Technology (OIT) concurs with the Office of Inspector General (OIG) recommendation that inventory management needs improvement. Changes since receipt of audit findings related to accountability (physical) management include: Inventory compliance as of February 28, 2022: 99.6%. Expected compliance level: 95%. Full compliance has been met. Inventory of physical assets will continue using perpetual updates to the inventory system of record to maintain at or above the compliance level of 95% for items updated within the last 365 days. Corporate Data Warehouse is the system of record for system component inventory of physical hardware assets.

Changes since receipt of audit findings related to visibility (logical) management include: VA has updated the Consolidated Mail Outpatient Pharmacy (CMOP) accreditation boundary to include infrastructure and storage devices, to facilitate scanning and vulnerability remediation based on Internet Protocol (IP) range and help prevent duplicate accounting of assets in the electronic Enterprise Mission Assurance Support System (eMASS) inventory. eMASS is the system inventory of accredited information systems/Authority to Operate boundaries. Forescout is the VA tool used for visibility (logical) reporting to network connected devices.VA OIT requests removal or closure of Recommendation 1.Supporting evidence is provided in Appendix A, Recommendation 1.

Recommendation 2: The OIG recommends the Tucson CMOP director implement more effective vulnerability and flaw remediation program that can accurately identify vulnerabilities and enforce flaw remediation.

Comments: Non-Concur. VA OIT non-concurs with OIG’s 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 at the Tucson CMOP of 92% for all critical and high vulnerabilities. The OIG scan data was ingested into the OIT vulnerability management tracking tool and that comparison demonstrated that OIT had the same vulnerabilities with a 2% variance due to the time difference when the scans were conducted.

VA OIT is continuously remediating and managing all vulnerabilities through mitigation efforts and Plan of Action and Milestones. OIT is currently in the process of implementing the next level of maturity with the establishment of enterprise risk tolerance for vulnerability management.

VA consistently maintains 90% or greater vulnerability management of all critical and high vulnerabilities across the enterprise. These statistically high percentages provide significant evidence that VA has implemented and is managing an effective Vulnerability Management and Flaw Remediation Program and aligned with federal and industry standards.

Recommendation 3: The OIG recommends the Tucson CMOP director 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.

Comments: Concur. VA concurs with OIG's recommendation to develop and implement methods to ensure delivery, receipt and understanding of assigned roles and responsibilities for CMOP activities. Tucson CMOP utilizes enterprise Change Management board through ServiceNow, which enforces approved implementation methods, receipts and understanding of roles and responsibilities. Tucson has updated the configuration management plan and updated the CMOP accreditation boundary to include infrastructure and storage devices, to facilitate scanning and vulnerability remediation based on IP range and help prevent duplicate accounting of assets in electronic eMASS inventory.

VA OIT requests removal or closure of Recommendation 3. Supporting evidence is provided in Appendix A, Recommendation 3.

Recommendation 4: The OIG recommends the Tucson CMOP director develop and implement a disaster recovery plan and capability that will restore operations in the event of a disruption to critical operations.

Comments: Concur. OIG stated Tucson CMOP needed a Disaster Recovery Plan (DRP) for CMOP Pharmaceutical Systems and Tucson CMOP. In the event of a catastrophic failure and total loss of their networking environment, Tucson CMOP has a DRP, but it does not meet recovery time objective. We are building the DRP site to meet this requirement. VA OIT has Identified this deficiency and a current Plan of Action and Milestones to resolve was submitted in Fiscal Year 2020. VA Cloud Team and National CMOP Management is currently working to build out a DRP site solution.

Target Completion Date: June 30, 2022.

Recommendation 5: The OIG recommends the Tucson CMOP director task the facility manager to change the default username and password for the security camera system.

Comments: Concur. Default username and password for security systems have been updated to meet security requirements. All new systems will be setup in accordance with VA security login procedures.

VA OIT requests removal or closure of Recommendation 5. Supporting evidence provided in Appendix A, Recommendation 5.

Recommendation 6: The OIG recommends the Tucson CMOP director request that OIT to configure audit logging on the misconfigured devices in accordance with established baselines, policy, and procedures.

Comments: Concur. VA's logging standard only applies to Server systems. Enterprise logging does not apply to end user type devices to include local facility automation systems. Tucson CMOP had Splunk Universal Forwarder installed and functioning on the nine servers on March 1, 2022.

Manual checks by the local site were done to confirm logging was in place for the servers in question. Results indicated that some of the IPs were no longer live, some were clusters consolidated back to the original active hosts, and the remaining active hosts were confirmed logging to Splunk.

The remainder 282 are workstations, laptops, mobile phones, building automation, printers, keyboard, video monitor, mouse, network devices and inactive IPs.

Target Completion Date: Completed. VA OIT requests removal or closure of Recommendation 6.

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 Luis Alicea Tom Greenwell Shawn Hill Jack Henserling Adam Sowells
Other Contributors	Jill Russell

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, Tucson CMOP

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
U.S. Senate: Mark Kelly, Kyrsten Sinema
U.S. House of Representatives: Andy Biggs, Ruben Gallego, Paul Gosar, Raul Grijalva, Ann Kirkpatrick, Debbie Lesko, Tom O'Halleran, David Schweikert, Greg Stanton

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