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 Dallas, Texas

INFORMATION TECHNOLOGY INSPECTION

REPORT # 21-03305-139

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.

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

www.va.gov/oig/hotline

1-800-488-8244

Executive Summary

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

The fiscal year (FY) 2020 FISMA audit indicated that VA continues to face significant challenges meeting the law's requirements. The 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.

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 in the sample for the annual audit required by FISMA or at facilities that previously performed poorly.

The OIG conducted this inspection to determine whether the Dallas Consolidated Mail Outpatient Pharmacy (CMOP) was meeting federal security guidance. The OIG selected the Dallas facility because it had not been previously visited as part of the OIG's annual FISMA audit. The inspection scope and methodology are described in appendix C.

What the Inspection Found

The OIG inspections are focused on four security control areas that apply to local facilities and have been selected based on their level of risk:

[1] Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014).

[2] Joint Task Force, *Security and Privacy Controls for Federal Information Systems and Organizations,* NIST Special Publication 800-53, rev. 5, 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.

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 Dallas CMOP Had Deficiencies in Five Configuration Management Controls

According to the Government Accountability Office's (GAO) *Federal Information System Controls Audit Manual*, configuration management identifies and controls IT hardware and software security features. The Dallas 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.
- **Flaw remediation** is how organizations correct software defects and often includes system updates, such as security patches.[9]

[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.

[9] NIST, *Guide for Security-Focused Configuration Management of Information Systems*, NIST Special Publication 800-128, August 2011; VA Handbook 6500, *Risk Management Framework for VA Information Systems-Tier 3: VA Information Security Program*, March 2015. VA HDBK 6500, March 2015, was in effect for the first five months of the time covered under this inspection and was superseded by a newer version in February 2021.

- **Configuration management plans** identify roles and responsibilities, resources, and processes to ensure any changes are evaluated and approved before implementation.
- **Baseline configurations** are documented, formally reviewed, and agreed upon-specifications that serve as a basis for future builds, releases, or changes to systems and include security and privacy control implementation.[10]

The Dallas CMOP did not have accurate inventories, despite OIT and VA's use of automated systems to maintain inventories of its system. A complete, accurate, and up-to-date inventory is required to implement an effective security program. Inaccurate component inventories affect vulnerability management effectiveness.

The OIG determined that OIT's vulnerability identification process and scans were ineffective. OIT scans for vulnerabilities routinely, randomly, and when new vulnerabilities are identified and reported. Although the inspection team and OIT used the same vulnerability scanning tools, OIT did not detect all the vulnerabilities that the team did. Some of the vulnerabilities were present on multiple computers. The inspection team identified 56 vulnerabilities—22 critical vulnerabilities on 62 computers and 34 high-risk vulnerabilities on 328 computers—which were not mitigated within the time frames established by OIT. The OIG also found 13 critical vulnerabilities and 16 high-risk vulnerabilities that OIT did not detect. While the agency is aware of many of the vulnerabilities, the plan of actions and milestones did not always list a remediation.[11]

Poor component inventories and poor 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 OIG 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 roles and responsibilities identified in the approved CMOP configuration plan were not implemented as planned. For example, the CMOP Change Implementation Board was not developed, resulting in a lack of centrally managed life cycle configuration management activities supporting the Dallas CMOP system.

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

[11] Plans of action and milestones identify tasks needing to be accomplished and details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. It also describes the measures planned to correct deficiencies identified in the controls and to address known vulnerabilities or security and privacy risks.

Over a third of the Dallas CMOP network equipment did not use operating systems that met VA baseline configurations. Further, the deficient devices were using operating systems past their vendor support dates, meaning they would not receive maintenance or vulnerability support. Network devices and IT systems are an organization's most critical infrastructure. Upgrading is not just a defensive strategy but a proactive one that protects the stability of the network. The baselines configurations for the network equipment are established by the VA OIT Configuration Control Board.

No Deficiencies Were Identified for Contingency Planning or Security Management Controls

The inspection team did not identify significant deficiencies in the controls implemented for contingency planning or security management at the Dallas CMOP.

The Dallas CMOP Had Six Deficiencies in Access Controls

According to the Government Accountability Office's *Federal Information System Controls Audit Manual* (FISCAM), access controls provide reasonable assurance that access to computer resources (data, equipment, and facilities) is restricted to authorized individuals. The Dallas 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.
- **Device lock** is a temporary action taken to prevent access to systems when users stop work or temporarily move away.
- **Identification and authentication** controls distinguish one user from another and establish the validity of a user's claimed identity.
- **Audit and monitoring** involves 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.[12]
- **Media sanitization** is the process of removing information from system media so that it cannot be retrieved or reconstructed.

[12] NIST Special Publication 800-128; VA Handbook 6500. VA HDBK 6500, March 2015, was in effect for the first five months of the time covered under this inspection and was superseded by a newer version in February 2021.

- **Physical access** involves restricting access to computer resources and protecting them from intentional or unintentional loss or impairment.

The OIG inspection team discovered the use of a single user administration account shared among multiple local OIT members for accessing production and other servers. This account has full elevated privileges to access, update, change, and remove systems. This account is required to run local software needed to run processes for the CMOP production equipment. Local managers were unable to determine who authorized the account as it was set up before they came to the facility. Further, OIT's access request system has no record of who authorized the account. Shared or group accounts have increased risk due to the lack of accountability. Instead, individual users should be uniquely identified. Further, the loss of accountability and integrity associated with this shared user account also affects other controls such as least privilege.[13]

During a routine walk-through, the OIG inspection team found a terminal that controls the production servers and conveyor system unlocked and unattended in the warehouse. Users failed to lock the workstation after performing maintenance on the production equipment. Numerous VA employees and contractors had physical access to the workstation. When no longer used, the workstation should be locked by a user or an administrator to prevent unauthorized access and changes to network resources. Failure to lock the workstation allows anyone with physical access the ability to gain unauthorized access to network resources, such as control of production and conveyor equipment. This access could result in disruption to operations.

The OIG identified databases that allow passwords that are not complex or are not periodically changed in accordance with VA identification and authentication policy requirements. Scan results also indicated that CMOP servers allowed local credentials for authentication. Additionally, abandoned user accounts were not removed from several servers, which could lead to misuse. Effects of misuse would be loss of protected health information or disruption of operations. VA complexity requirements were not enforced on databases, and some passwords were not set to expire on several servers. The personnel responsible for managing the servers indicated that they were aware of the security requirements; however, the plan of action and milestones to correct the authentication issue was not created until the OIG requested it. Weak password controls expose organizations to a greater risk of compromise. Once compromised, a local database account could be used for unauthorized disclosure or modification of prescription information.

The OIG inspection team identified deficiencies in logging administrative actions, log retention, and log reviews for databases at the Dallas CMOP. For instance, the team reviewed 20 event logs of administrative access and discovered that the logs were overwritten within minutes, which is

[13] Least privilege is a principle requiring that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use of an information system.

in violation of VA policy. The Dallas CMOP had not deployed a mechanism to copy the database's log files to long-term storage or prevent them from being overwritten. Logs frequently provide value during security incident analysis by recording which accounts were accessed and what actions were performed. If this information is not available, an investigation may be limited or unsuccessful in determining the unauthorized use or modification of CMOP information.

The CMOP did not meet the VA security standards for proper media sanitization. Local OIT personnel used a degaussing machine, which sanitizes hard drives removed from system devices as required by VA policy. Personnel also logged hard drives for removal and sanitization. However, they did not implement a verification process that validated and logged that the hard drives were sanitized, or that the action was effective prior to disposal. Effective sanitization techniques and tracking of storage media are critical aspects of ensuring that an organization's sensitive data is being protected against unauthorized disclosure. Since the CMOP OIT personnel did not validate sanitization, there is a risk of loss or disclosure of personally identifiable information on the hard drives. This could impact the organization's mission, damage organizational assets, and result in financial loss or harm to veterans.

The Dallas CMOP did not employ perimeter or parking barriers. The main entrance and administration offices are next to 12 parking stalls and the main road entrance, which do not have controlled access. VA policy restricts parking next to facilities and mandates physical barriers to prevent a vehicle attack on a facility.[14] Further, the Dallas VA Medical Center police department issued a report on January 22, 2021, to the facility director identifying a lack of physical barriers and parking standoff as a problem. When the OIG visited the site, no barriers or standoffs had been implemented. A lack of physical barriers and a parking area in proximity to the Dallas CMOP make the facility an easier target for vehicle-borne attacks that could result in the loss of life, assets, and critical information.

What the OIG Recommended

The OIG made 10 recommendations to the Dallas Consolidated Mail Outpatient Pharmacy director:

1. Implement an effective inventory management system for all network segments.
2. Implement an 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.

[14] VA Physical Security and Resiliency Design Manual, chap. 3, sec. 3.3, "Standoff Distance," October 1, 2020, rev. September 1, 2021.

4. Implement effective configuration control processes that ensure network devices comply with security standards mandated by the VA OIT Configuration Control Board.
5. Remove or disable group accounts to comply with established VA security requirements and policy.
6. Ensure employees lock devices when they are unattended.
7. Implement a method of database authentication that complies with NIST standards and VA security requirements.
8. Develop and implement a process to retain database logs for a period consistent with VA's record retention policy.
9. Establish a process for validating and logging the sanitization of hard drives.
10. Implement parking barriers that meet VA Physical Security & Resiliency Design Manual requirements.

VA Comments and OIG Response

The assistant secretary for information and technology and chief information officer provided comments for the Dallas CMOP. The assistant secretary concurred with recommendation 1, and recommendations 3 through 10. The assistant secretary requested recommendations 3, 4, 6, 7, and 9 be closed due to corrective actions he said were completed.

The assistant secretary 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 96 percent for all critical and high vulnerabilities at the Dallas CMOP. The assistant secretary also stated that VA consistently maintains a 90 percent or greater vulnerability management rate for all critical and high vulnerabilities across the enterprise. The assistant secretary believes this demonstrates that OIT has implemented and is managing an effective vulnerability and flaw remediation program aligned with federal and industry standards.

Regarding the nonconcurrence with recommendation 2, the assistant secretary did not provide evidence that would allow OIG to validate the assertion that it demonstrated vulnerability identification, remediation, mitigation, and management rates of 96 percent for all critical and high vulnerabilities. Contrary to this assertion, OIT's own results indicated that only 56 percent of the critical vulnerabilities had completed remediations. The remaining vulnerabilities either had corresponding plans of action and milestones and were awaiting action or had no status to report. For the high vulnerabilities, OIT reported that only 48 percent had completed remediation and almost 48 percent were awaiting updates. Furthermore, the OIG identified 22 critical

vulnerabilities within its vulnerability scans while OIT scans identified 11, which is 50 percent less than the OIG. The OIG also identified 34 high vulnerabilities while OIT scans identified 22, which is 35 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.

The assistant secretary provided responsive actions plans for the nine recommendations with which he concurred. Based on evidence provided, the OIG considers recommendations 3, 4, 6, 7, and 9 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
Assistant Inspector General
for Audits and Evaluation

Contents

Abbreviations

CMOP	Consolidated Mail Outpatient Pharmacy
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Modernization Act
FY	fiscal year
GAO	Government Accountability Office
IT	information technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information and Technology

Introduction

The VA Office of Inspector General (OIG) conducted this inspection to determine whether the Dallas Consolidated Mail Order Pharmacy (CMOP) was meeting federal security requirements and complying with related guidance.[15] The inspection team selected the Dallas CMOP because it had not been previously visited as part of the OIG's annual Federal Information Security Modernization Act (FISMA) audit.

FISMA was established, in part, to improve oversight of federal agency information security programs.[16] The law requires VA to 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. To determine compliance with FISMA, the OIG contracts with an independent public accounting firm that conducts an annual audit of VA's information security program and practices.

In 2020, the OIG started an information technology (IT) security inspection program. Security inspections assess the effectiveness of controls that protect VA systems and data from unauthorized access, use, modification, or destruction. Inspections provide recommendations to VA on enhancing information security oversight at local facilities.[17] The OIG IT inspections review sites not evaluated under the annual FISMA audits, which only inspect a sample, or facilities that did not perform well in prior FISMA audits. The OIG's IT inspections are not intended to duplicate FISMA audits. However, there is some redundancy in that some of the controls are assessed for both inspections and audits 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, as shown in table 1.

[15] Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. No. 113-283, 128 Stat 3073 (2014); National Institute of Standards and Technology guidance; VA's IT security policies.

[16] FISMA. See appendix B for additional information about FISMA.

[17] 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 by the OIG

Control area	Purpose	Examples evaluated
Configuration Management	Identify and manage security features for all hardware and software components of an information system	Component inventory, baseline configurations, configuration settings, change management, vulnerability management, and flaw remediation
Contingency Planning	Provide reasonable assurance that information resources are protected and 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	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	Provide reasonable assurance that computer resources are restricted to authorized individuals	Access, identification, authentication, audit, and accountability including related physical security controls

Source: FISCAM.

Without these critical controls, VA's systems are at risk of unauthorized access or modifications. 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 requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system.[18]

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

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

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

Office of Information and Technology Structure and Responsibilities

The assistant secretary for information and technology and chief information officer leads the Office of Information and Technology (OIT). 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. The Cybersecurity Operations Center is part of OIT's Office of Information Security. It is responsible for protecting VA information and information systems by identifying and reporting emerging and imminent threats and vulnerabilities. OIT's Office of Development, Security, and Operations unifies software development, software operations, service management, information assurance, cybersecurity compliance, performance monitoring, and technical integration throughout the entire solution delivery process, as shown in figure 1.

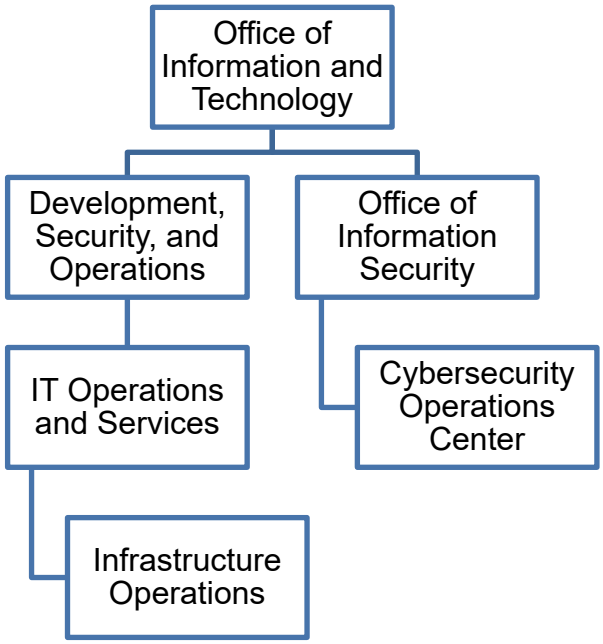

Figure 1. *Organizational structure of Office of Information and Technology entities relevant to this inspection.*
Source: VA OIG analysis.

OIT's Information Technology Operations and Services Office provides standardized customer service, technology implementation, and technical support. According to its mission statement, Infrastructure Operations is focused on efficiently delivering secure and high-availability

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

infrastructure solutions in support of VA's mission. OIT assigns dedicated Infrastructure Operations personnel to the Dallas CMOP.

Results of Previous Projects

The OIG issues annual reports on VA's information security program. The FISMA audit is conducted in accordance with guidelines issued by the Office of Management and Budget and applicable National Institute of Standards and Technology (NIST) information security guidelines.[20] The FY 2020 FISMA audit, conducted by CliftonLarsonAllen LLP, an independent public accounting firm, 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.[21] 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.[22] Repeat recommendations included addressing deficiencies in configuration management, contingency planning, security management, and access controls.

A November 2019 Government Accountability Office (GAO) review found that VA continued to have a deficient information security program.[23] 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.

[20] Joint Task Force, *Security and Privacy Controls for Federal Information Systems and Organizations,* NIST Special Publication 800-53, rev. 5, September 2020, includes updates as of Dec. 10, 2020.

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

[22] 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.

[23] 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."[24]

Dallas CMOP

VA's Pharmacy Benefits Management Services operate the CMOPs, including the one in Dallas. Combined, the VA CMOPs processed 125 million prescriptions in FY 2019—about 80 percent of Veterans Health Administration outpatient prescriptions—along with prescriptions for 74 Indian Health Service sites and VA's Civilian Health and Medical Program.

The Dallas CMOP facility is about 90,000 square feet and services VA medical sites in Arizona, Arkansas, Louisiana, Mississippi, Oklahoma, and Texas. The CMOP's projected FY 2021 expenses are over $768 million, and it processed over 19 million prescriptions in FY 2020.

Figure 2. *Dallas Consolidated Mail Order Pharmacy.*
Source: VA OIG inspection team, September 15, 2021.

[24] 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 Dallas CMOP. Two of these areas had deficiencies.

In configuration management, the team identified deficiencies with component inventory, vulnerability management, flaw remediation, baseline configurations, and implementation of the configuration management plan.

The inspection team did not identify deficiencies in contingency planning controls. The review showed that VA's policies and procedures addressed control criteria such as identifying critical operations, implementing environmental controls, and performing preventative maintenance.

Similarly, during the evaluation of security management controls, the team did not identify deficiencies in 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, device lock, identification and authentication, audit and monitoring, media sanitization, and physical security controls.

I. Configuration Management Controls

According to the GAO's *Federal Information System Controls Audit Manual* (FISCAM), configuration management involves identifying and managing security features for all hardware, software, and firmware components of an information system at a given point and systematically controlling changes to that configuration during the system's life cycle.[25] The inspection team reviewed and evaluated the 12 configuration management controls drawn from NIST criteria for VA-hosted systems at the Dallas CMOP to determine if they met federal guidance and VA requirements.

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 should first establish an accurate component inventory to identify all computers on the network. The component inventory affects the success of other controls, such as vulnerability and patch management. OIT's Cybersecurity Operations Center identifies and reports threats and vulnerabilities for VA. Once this process is complete, OIT's Patch and Vulnerability Team develops procedures to remediate identified issues, which may include applying patches. This process helps secure computers from attack.

[25] GAO, FISCAM. FISCAM configuration management critical elements are listed in appendix B.

Finding 1: The Dallas CMOP Had Deficiencies in Five 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 system change management processes; reviewed local policies, procedures, and inventory lists; and scanned the Dallas CMOP's network to identify devices. The team compared the devices found on the network with the device inventories found in VA's information system assessment and authorization software tool; the team also received vulnerability lists provided by OIT and scanned the Dallas CMOP's network to identify vulnerabilities.[26] Both the 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; or
- remediate flaws including unsupported versions of applications, missing patches, and vulnerable plug-ins.

Additionally, the inspection team found problems with the CMOP's

- configuration management plan, and
- baseline configurations.

By not implementing more-effective configuration management controls, VA is placing critical systems at unnecessary risk of unauthorized access, alteration, or destruction.

Component Inventory

Previous FISMA reports have repeatedly identified inventory deficiencies as a nationwide issue for VA. Component inventories are descriptive records of IT assets in an organization down to the system level. A complete, accurate, and up-to-date inventory is required to implement an effective information security program because it provides greater visibility into and control over these systems.[27] The inspection team identified inaccuracies in the component inventory at the Dallas CMOP, despite OIT and VA's use of automated systems to maintain inventories of its information systems. VA identified 257 devices in the CMOP's inventory. However, the OIG team identified 355 devices. In total, the team identified 98 more devices than were accounted for by the local system authorization to operate and 141 total discrepancies between the accreditation package and scan data. Additionally, the team identified 11 operational devices for

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

the Real Time Location System that were not identified in its accreditation. The team also identified nine physical access control systems and 167 security camera devices that were not authorized to be connected to the network.

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 Dallas CMOP. According to GAO, "Vulnerability assessments involve analyzing a network to identify potential vulnerabilities that would allow unauthorized access to network resources, simulating what might be performed by someone trying to obtain unauthorized access."[28] Vulnerability management is the process by which OIT identifies, classifies, and reduces weaknesses and is part of assessing and validating risks as well as monitoring the effectiveness of a security program. The Cybersecurity Operations Center identifies and reports threats and vulnerabilities for VA, and OIT conducts scans for vulnerabilities routinely, randomly, or when new vulnerabilities are identified and reported.

However, OIT's vulnerability management controls did not effectively identify weaknesses in its network. For example, the inspection team identified vulnerabilities such as operating systems that were no longer vendor supported and applications with missing security 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.

NIST assigns severity levels to vulnerabilities by using the Common Vulnerability Scoring System, a framework for communicating the characteristics of software vulnerabilities.[29] The 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 vulnerability management processes. For example, on a scale of zero to 10, critical vulnerabilities have a score between 9.0 and 10, while high-risk vulnerabilities have a score between 7.0 and 8.9. OIT establishes time frames for remediating vulnerabilities based on their severity.

The inspection team compared OIT-provided network vulnerability scan results from the Dallas CMOP against scans conducted by the OIG team from September 13 to September 17, 2021. The team and OIT used the same vulnerability scanning tools. The team identified 56 vulnerabilities (22 critical vulnerabilities on 62 computers and 34 high vulnerabilities on 328 computers) that

[28] GAO, FISCAM: A vulnerability is a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source."

[29] "Vulnerability Metrics," NIST National Vulnerability Database, accessed January 28, 2022, https://nvd.nist.gov/vuln-metrics/cvss; "Common Vulnerability Scoring System ver. 3.14, Specification Document, Revision 1," accessed January 28, 2022, https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf.

were not mitigated within the time frames established by OIT. Moreover, OIT's security scans were inadequate because the team found 13 critical vulnerabilities and 16 high-risk vulnerabilities that OIT did not detect. While the agency is aware of many of the vulnerabilities, the plan of actions and milestones did not always list a remediation.[30] The OIG identified critical and high vulnerabilities on approximately17 percent of the devices at the Dallas CMOP.

Unidentified threats cannot be mitigated; therefore, they represent weaknesses that could be exploited to gain access to VA data. Consequently, management personnel should periodically perform assessments to protect information, address vulnerabilities, and make decisions about accepting or mitigating risks.[31]

Flaw Remediation

The Dallas 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. Flaw remediation is the process by which organizations correct software defects, including applying updates such as patches. Security patches are usually the most effective way to mitigate software flaw vulnerabilities and are often the only fully effective solution. According to GAO, a patch is a piece of software code that is inserted into a program to temporarily fix a defect. 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.[32]

VA 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 uses 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 processes, the inspection team identified several devices that were missing security patches. Without an effective patch management program,

[30] Plans of action and milestones identify tasks needing to be accomplished. Then, it details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. It also describes the measures planned to correct deficiencies identified in the controls and to address known vulnerabilities or security and privacy risks.

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

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

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's authorization requirements standard operating procedures are developed to ensure systems obtain and maintain a VA authorization to operate.[33] These procedures provide guidance to information system security officers, owners, and 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 in accordance with the plan. For instance, the CMOP Change Implementation Board was not developed, resulting in a lack of centrally managed life cycle configuration management activities supporting the Dallas CMOP system. Without an implemented configuration management plan, VA cannot ensure that configuration policies are tailored to individual systems or that system changes are approved and managed during systems' lifecycle.

Baseline Configurations

The inspection team noted that over a third of the Dallas CMOP network equipment used operating systems that did not meet VA baseline configurations. Furthermore, the deficient devices were using operating systems that are past their support dates and will not receive maintenance or vulnerability support. Baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, or changes to systems that include security and privacy control implementation.[34] The baseline configurations for the network equipment are approved by the VA OIT Configuration Control Board. Network devices and IT systems are an organization's most critical infrastructure. Upgrading is not just a defensive strategy, but a proactive one that protects the network stability.

[33] Office of Information Security, "Authorization Requirements Standard Operating Procedures," ver. 1.24, May 13, 2021.

[34] NIST Special Publication 800-53.

Finding 1 Conclusion

The Dallas CMOP did not have accurate inventories, a problem that led to undetected and unaddressed critical and high-risk vulnerabilities in its systems. Its vulnerability management controls did not effectively identify network weaknesses such as unsupported versions of applications, and its flaw remediation controls did not ensure comprehensive patch management. The Dallas CMOP configuration management plan was not fully implemented, preventing key personnel from providing expected capabilities and functions, and old operating systems no longer met baseline configurations. 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 1–4

The OIG made the following recommendations to the director of the Dallas Consolidated Mail Order Pharmacy:

1. Implement an effective inventory management system for all network segments.
2. Implement an 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 local activities to ensure full implementation of approved policy.
4. Implement effective configuration control processes that ensure network devices maintain standards mandated by the VA Office of Information and Technology Configuration Control Board.

Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 1, 3, and 4. The assistant secretary reported OIT is in the process of implementing physical and logical inventory changes that will result in the CMOP complying with inventory requirements. The assistant secretary also reported that the CMOP has updated the configuration plan to remediate the OIG finding and to meet VA regulations. The assistant secretary reported that VA updated the baseline version of the Internetwork Operating System to ensure network devices maintain configuration control board mandated standards.

The assistant secretary did not concur with recommendation 2. The assistant secretary reported that within the period of the inspection, OIT was able to demonstrate vulnerability identification, remediation, mitigation, and management rates of 96 percent for all critical and high vulnerabilities at the Dallas CMOP. The assistant secretary also stated that VA consistently maintains a 90 percent or greater vulnerability management rate for all critical and high

vulnerabilities across the enterprise. OIT believes this demonstrates 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 were in progress and were completed for recommendations 3 and 4. OIT provided sufficient evidence to support that the actions were completed. As a result, the OIG considers recommendation 3 and 4 closed. For recommendation 1, the 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 evidence demonstrating progress in addressing the issues identified.

Regarding the nonconcurrence with recommendation 2, the assistant secretary did not provide evidence that would allow OIG to validate the assertion that it demonstrated vulnerability identification, remediation, mitigation, and management rates of 96 percent for all critical and high vulnerabilities. Contrary to this assertion, OIT's own results indicated that only 56 percent of the critical vulnerabilities had completed remediations. The remaining vulnerabilities had corresponding plans of action and milestones and were awaiting action or had no status to report. For the high vulnerabilities, OIT reported that only 48 percent had completed remediation and almost 48 percent were awaiting updates. Further, the OIG identified 22 critical vulnerabilities within its vulnerability scans while OIT scans identified 11, which is 50 percent less than the OIG. The OIG also identified 34 high vulnerabilities while OIT scans identified 22, which is 35 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.

II. Contingency Planning Controls

Contingency planning for systems is part of an overall program for achieving continuity of operations for organizational mission and business functions. According to FISCAM, contingency planning controls provide reasonable assurance that controls are in place to protect information resources and 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.[35]

If contingency planning controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. To determine whether recovery plans will work as intended, they should be tested periodically in disaster-simulation exercises. FISMA requires that each federal agency implement an information security program that includes "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."[36] 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 fires, natural disasters, and terrorism, which would require reestablishing operations at a remote location. To determine if the Dallas CMOP met federal guidance and VA requirements, the inspection team evaluated 22 contingency planning controls.

Finding 2: No Weaknesses Were Found 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.

[35] GAO, FISCAM. The FISCAM critical elements for contingency planning are listed in appendix B.
[36] FISMA.

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. The team verified that the Dallas CMOP had an alternate processing facility, and that training, testing and exercise were conducted in accordance with policies. The team did not identify deficiencies in the Dallas CMOP's contingency planning controls. Accordingly, the OIG did not make any recommendations for improvement.

III. Security Management Controls

According to FISCAM, security management controls establish a framework and continuous cycle for assessing risk, developing security procedures, and monitoring the effectiveness of the procedures. The inspection team evaluated seven critical security management controls: instituting a security management program, assessing and validating risk, documenting and implementing security control policies and procedures, implementing security awareness and personnel policies, monitoring the program, remediating information security weaknesses, and ensuring third-party security.[37]

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 the authoritative management tool for VA's assessment and authorization process and risk management framework. Among the topics reviewed were security assessment, continuous monitoring strategy, risk analysis, and plan of action and milestones for known deficiencies. The team also interviewed information system security officers, local administrators, contracting officer's representatives, human resources staff member, privacy officers, and system stewards.

The Dallas 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 not identify any deficiencies in the Dallas CMOP's security management controls other than an unsigned policy. However, a signed copy was provided during the review. Accordingly, the OIG did not make any recommendations for improvement.

[37] FISCAM critical elements for security management are listed in Appendix B.

IV. Access Controls

Previous FISMA reports have repeatedly identified access controls as a nationwide issue for VA. According to FISCAM, 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 Dallas CMOP, the inspection team reviewed all six critical access control elements.[38]

Finding 4: The Dallas CMOP Had Deficiencies in Six Access Controls

To evaluate the Dallas CMOP's access controls, the inspection team interviewed the information system security officer, system steward, local administrators, and the system owner; reviewed local policies and procedures; conducted a walk-through of the facility; and analyzed audit logs.[39]

The OIG found these problems with access controls at the Dallas CMOP:

- One administrative account with elevated privileges was shared by several users.
- Users failed to lock workstations after performing maintenance.
- Application owners used weak password controls for local databases.
- Database managers did not adequately maintain log data for local databases.
- Local administrators did not verify media sanitization resulted in unrecoverable information.
- The director did not employ perimeter or parking barriers.

Account Management

The Dallas CMOP did not meet the criteria for maintaining accountability for administration-user accounts. Account management is the process of requesting, establishing, issuing, and closing user accounts; tracking users and their respective access authorizations; and managing these functions.[40] The OIG inspection team discovered a single user administration account being shared among multiple local OIT members for accessing production and other servers. This account has full elevated privileges to access, update, change, and remove systems. This account is required for local software needed to run CMOP production equipment processes. A system administrator identified this account as a "Service Account." However, that

[38] FISCAM critical elements for access controls are listed in Appendix B.

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

[40] GAO, FISCAM.

description was incorrect as the account was missing several qualities that apply to a service account. Local management was unable to determine who initially authorized the account. Further, OIT's access request system has no record of who authorized the account. Information system security officers perform monthly audits to identify accounts with elevated privileges. However, this account was not identified in the audit conducted before the inspection. Shared or group accounts have increased risk due to the lack of accountability; instead, accounts should have uniquely identified, individual users. The loss of accountability and integrity associated with this shared user account also affects other controls, such as least privilege.[41]

Device Lock

During a walk-through, the OIG inspection team found a terminal that controls the production servers and conveyer system unlocked and unattended in the warehouse. Numerous VA employees and contractors had physical access to the workstation. Device lock is a temporary action take to prevent access to systems when users stop work or temporarily move away. When no longer being used, a workstation should be locked by a user or administrator. Failure to lock the workstation allows anyone with physical access to the workstation the ability control production equipment and potentially disrupt operations. Further, the account had escalated privileges that could allow installation of malicious software.

Identification and Authentication

The OIG identified databases that allow passwords that are not complex or are not periodically changed in accordance with VA information security policy. The inspection team's scan results also indicated that the CMOP servers allow local credentials that rely on weak, single-factor authentication to provide system access. Additionally, abandoned user accounts are not removed from several servers, a lapse that violates VA policy and could lead to misuse. Identification and authentication controls distinguish one user from another and establish the validity of a user's claimed identity.[42] Effects of misuse would be loss of protected health information or disruption of CMOP operations. VA complexity requirements were not enforced on databases, and some passwords were not set to expire on several servers in accordance with VA policy. Interviews with the person responsible for managing the servers indicated that complex and periodically changed passwords cannot be enforced as the CMOP application uses hard-coded passwords. Database personnel also indicated that they were aware of the security requirements; however, the plan of action and milestones to correct the authentication issue was not created until the OIG requested it. Weak password controls expose organizations to a greater risk of compromise.

[41] Least privilege is a principle requiring that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use of an information system.

[42] GAO, FISCAM.

Once compromised, a local database account could be used for unauthorized disclosure or modification of prescription information.

Audit and Monitoring

The OIG determined that improvements are needed for logging of administrative actions, log retention, and log reviews for databases at the Dallas CMOP. 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.[43] The inspection team reviewed 20 different event logs that recorded administrative access and discovered that the logs were overwritten within minutes. The team also ran security scans, which indicated that settings on a server did not have adequate controls against overwriting logs. The Dallas CMOP had not deployed mechanisms to copy database log files to long-term storage or prevent them from being overwritten. Logs frequently help with incident analysis. They provide information such as which accounts were accessed and what actions were performed. If this information is not available, an investigation may be limited or unsuccessful in determining the unauthorized use or modification of information.

Media Sanitization

The Dallas CMOP did not meet the criteria for a proper media sanitization process. Media sanitization is the process of removing information from system media so that it cannot be retrieved or reconstructed. Although local OIT personnel used a degaussing machine, which sanitizes hard drives removed from system devices, and personnel logged hard drives for removal and sanitization as required by VA policy, personnel did not implement a verification process to validate and log that the hard drives were sanitized or that the action was effective prior to disposal. Effective sanitization techniques and tracking of storage media are critical aspects of ensuring that sensitive data is protected against unauthorized disclosure. Attackers may attempt to obtain sensitive information by retrieving residual organizational data on media that was not properly sanitized.[44]

Since local OIT personnel did not validate sanitization, there is a risk of loss or disclosure of personally identifiable information on the hard drives. This could endanger the organization's mission, damage organizational assets, and result in financial loss or harm to veterans.

[43] GAO, FISCAM.

[44] NIST Special Publication 800-88 revision 1.

Physical Access

The Dallas CMOP did not employ perimeter or parking barriers. For example, the main entrance and administration offices are directly next to 12 parking stalls and the main road entrance, which does not have controlled access. Physical access controls restrict access to computer resources, protecting them from intentional or unintentional loss or impairment. VA policy restricts parking next to facilities and mandates physical barriers to prevent a vehicle attack on a facility.[45] Further, the Dallas VA Medical Center police department issued a report on February 21, 2021, to the director identifying a lack of physical barriers and parking standoff as a problem. When the OIG visited the site, no barriers or standoffs had been implemented. When the OIG asked if the facility had plans to implement the controls, managers responded that it was not an IT issue. A lack of physical barriers and parking area in proximity to the facility make it an easier target for a vehicle-borne or explosive attack that could result in the loss of life, assets, and critical information.

Finding 4 Conclusion

The Dallas CMOP was using a shared user account with elevated privileges, which reduces accountability and weakens other controls. Additionally, CMOP personnel did not lock their workstations while unattended, databases at the CMOP were using weak password controls, database audit logs were not properly retained, media sanitization was not being validated at the facility, and barriers were not put up to reduce the risk of vehicle-borne attacks. Unless the CMOP takes corrective actions, it risks unauthorized access to critical network resources, inability to respond effectively to incidents, loss of personally identifiable information, and even loss of life.

Recommendations 5–10

The OIG made the following recommendations to the director of the Dallas Consolidated Mail Order Pharmacy:

5. Remove or disable group accounts to comply with established requirements and criteria.
6. Ensure employees lock devices when they are unattended.
7. Implement database authentication processes that comply with National Institute of Standards and Technology standards and VA security requirements.
8. Implement a process to retain database logs for a period consistent with VA's record retention policy.

[45] VA Physical Security and Resiliency Design Manual chap 3., sec 3.3, "Standoff Distance" October 1, 2020, rev. September 1, 2021.

9. Establish a process for validating and logging the sanitization of hard drives.
10. Implement parking barriers that meet VA Physical Security & Resiliency Design Manual requirements.

Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 5 through 10. The assistant secretary reported that the Dallas CMOP information technology department is working with the vendor to perform analysis of the effect on the system. The assistant secretary reported that briefings, security checks, and training have been conducted to ensure employees lock devices. The assistant secretary reported that the database team has remediated the password and database scan issues. OIT is also installing an agent on all database servers as part of an audit logging and retention project. The assistant secretary reported that staff were training on the media destruction program that outlines media sanitization processes. Finally, the assistant secretary reported that the Dallas CMOP will work with the Veterans Health Administration to complete a risk assessment of the site and will have a plan in place to fix or accept the risks.

OIG Response

The assistant secretary reported the corrective actions regarding recommendations 6, 7, and 9 were completed and provided sufficient evidence to support his assertion. As a result, the OIG considers these three recommendations closed. The assistant secretary reported the corrective actions regarding recommendations 5, 8, and 10 were in progress. The OIG will monitor implementation of the planned actions and will close the recommendations when VA provides evidence demonstrating progress in addressing the issues identified.

Overall Conclusion

The inspection team identified deficiencies in component inventory, vulnerability management, flaw remediation, baseline configurations, configuration management planning, account management, device lock, identification and authentication, audit and monitoring, media sanitization, and physical security controls. The OIG made 10 recommendations to the director of the Dallas CMOP: (1) implement an effective inventory management systems for all network segments; (2) implement an effective vulnerability and flaw remediation program that can accurately identify vulnerabilities and enforce flaw remediation; (3) implement methods to ensure delivery, receipt, and understanding of assigned roles and responsibilities for local activities to ensure full implementation of approved policy; (4) implement effective configuration control processes that ensure network devices maintain VA OIT Configuration Control Board mandated standards; (5) remove or disable group accounts to comply with established requirements and criteria; (6) enforce proper access control practices; (7) implement

a method of database authentication that complies with NIST and VA requirements; (8) implement a process to retain database logs for a defined period consistent with VA's record retention policy; (9) establish a process for validating and logging the sanitization of hard drives; and (10) implement parking barriers that meet VA Physical Security & Resiliency Design Manual requirements.

Although the information and recommendations in this report are based on findings specific to the Dallas 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 Dallas 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 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 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.

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 identifying, naming, and describing physical and functional characteristics of a controlled item, as well as performing activities to define, track, store, manage, and retrieve configuration items. Examples of these controls are baseline configurations, configuration settings, and component inventories.
- **Authorize, test, approve, and track changes** by formally establishing a change management process, with management's authorization and approval of the changes. This element includes documenting and approving test plans, comprehensive and appropriate testing of changes, and creating an audit trail to clearly document and track changes.
- **Conduct routine configuration monitoring** to determine the accuracy of the changes that should address baseline and operational configuration of hardware, software, and firmware.[46] 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

[46] 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.

restrictions, user-installed software, malicious code protection, security alerts, and advisories. Examples of controls in this element are vulnerability scanning, flaw remediation, malicious code protection, security alerts, and advisories.

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

FISCAM identifies the following critical elements for contingency planning:

- **Computerized operations criticality and sensitivity assessment** is an analysis of data and operations by management to determine which are the most critical and what resources and needed to recover and support them.
- **Prevent and minimize damage and interruption** by implementing backup procedures and installing environmental controls. These controls are generally inexpensive ways to prevent relatively minor problems from becoming costly disasters. This control also includes effective maintenance, problem management and change management for hardware.
- **A comprehensive contingency plan** or suite for related plans, should be developed for restoring critical applications; this includes arrangements for alternate processing facilities in case the usual facilities are damaged or cannot be accesses.
- **Contingency testing** determines whether they will function as intended and can reveal important weaknesses which leads to plan improvement.

FISCAM has seven critical elements for security management:

- **Institute a security management program** that establishes policies, plans, and procedures clearly describing all major systems and facilities and that outlines the duties of those responsible for overseeing security as well as those who own, use, or rely on the organization's computer resources. There should be a clear security management structure for systems and devices as well as for business processes. Examples of specific controls are system security plans, plan updates, activity planning, and resource allocation.
- **Assess and validate risk** by comprehensively identifying and considering all threats and vulnerabilities. This step ensures that agencies address the greatest risks and appropriately decide to accept or mitigate risks. Examples of these controls are security certification, accreditation, categorization, and risk assessment.

- **Document and implement security control policies and procedures** that appropriately address general and application controls and ensure users can be held accountable for their actions. These controls, which are more general at the entity-wide level and more specific at the system level, should be approved by 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 operating effectively. Examples of these controls are security assessments, continuous monitoring, privacy impact assessments, and vulnerability scanning.
- **Remediate information security weaknesses** when they are identified, which involves reassessment of related risks, applying appropriate corrective actions, and follow-up monitoring to ensure actions are effective. Agencies develop plans of actions and milestones to track weaknesses and corresponding corrective actions.
- **Ensure third parties are secure,** as vendors, business partners, and contractors are often granted access to systems for purposes such as outsourced software development or system transactions.[47]

FISCAM lists six access control critical elements:

- **Boundary protection controls** protect a logical or physical boundary around a set of information resources and implement measures to prevent unauthorized information exchange across the boundary. Firewall devices are the most common boundary protection technology.
- **Sensitive system resources controls** are designed to ensure the confidentiality, integrity, and availability of system data such as passwords and keys during transmission and storage. Technologies used to control sensitive data include encryption and certificate management.

[47] GAO, FISCAM.

- **Physical security** restricts access to computer resources and protects them from loss or impairment. Physical security controls include guards, gates, locks, and environmental controls such as smoke detectors, fire alarms and extinguishers, and uninterruptible power supplies.
- **Audit and monitoring controls** involve the collection, review, and analysis of events for indications of inappropriate or unusual activity. These controls should be routinely used to assess the effectiveness of other security controls, to recognize an attack, and to investigate during or after an attack.
- **Identification and authentication controls** distinguish one user from another and establish the validity of a user's claimed identity.
- **Authorization controls** determine what users can do, such as granting access to various resources, and depend on valid identification and authentication controls. These controls establish the validity of a user's claimed identity.

Federal Information Security Modernization Act of 2014

The stated goals of FISMA are:

- 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.[48]

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

[48] FISMA.

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

NIST Information Security Guidelines

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

Appendix C: Scope and Methodology

Scope

The inspection team conducted its work from September 2021 through March 2022. When the team inspected the Dallas CMOP during the week of September 13, 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 facility staff and followed the Centers for Disease Control and Prevention's recommendations, including wearing masks. To further limit contact with facility 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 FISMA, NIST security guidelines, and VA's IT security policy. 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 the Dallas CMOP's 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.

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 appendix II as a guide to help develop evidence requests and a base set of interview questions for the Dallas CMOP and its personnel. The team used the FISCAM controls identified in appendix B as an overlay to correlate FISMA controls used by VA to protect and secure 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 Dallas 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 in the context of the audit objectives, could occur during this inspection. The team exercised due diligence in staying alert to any fraud indicators. The OIG did not identify any instances of fraud or potential fraud during this inspection.

Data Reliability

The inspection team generated computer-processed data by using network scanning tools. The results of the scans were provided to the 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: April 11, 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 Dallas, Texas, Project Number 2021-03305-AE-0167 (VIEWS 07188260)

To: 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 Consolidated Mail Outpatient Pharmacy in Dallas, Texas.

2. 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 Office of Inspector General Draft Report,

Inspection of Information Technology Security at the Consolidated Mail Outpatient Pharmacy in Dallas, Texas, Project Number 2021-03305-AE-0167 (VIEWS 07188260)

OIG Recommendation 1: Implement an effective inventory management system for all networks.

Comments: Concur. Changes since receipt of audit findings related to accountability (physical) management include inventory compliance as of February 28, 2022, at 98.1%. The expected compliance level is 95%, thus full compliance was 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 an updated Consolidated Mail Outpatient Pharmacy (CMOP) accreditation boundary, which includes 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 (ATO) boundaries. Forescout is the tool the Department uses for visibility (logical) reporting to network connected devices. The target completion date is June 29, 2022.

OIG Recommendation 2: Implement an effective vulnerability and flaw remediation program that can accurately identify vulnerabilities and enforce flaw remediation.

Comments: Non-Concur. Within the timeframe of the overall inspection, the Department of Veterans Affairs (VA), Office of Information and Technology (OIT) was able to demonstrate vulnerability identification, remediation, mitigation and management rates at the Dallas CMOP of 96% for all critical and high vulnerabilities. The Office of Inspector General (OIG) scan data was ingested into the OIT vulnerability management tracking tool and that comparison demonstrated that OIT had the same vulnerabilities with a 3.27% variance due to the time difference of when the scans were conducted.

VA OIT is continuously remediating and managing all vulnerabilities through mitigation efforts and Plans of Action and Milestones (POAM). 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 in alignment with federal and industry standards. Supporting evidence provided in Appendix A, Recommendation 2. [The OIG did not include the appendix referenced here as part of this report.]

OIG Recommendation 3: Develop and implement methods to ensure delivery, receipt, and understanding of assigned roles and responsibilities for local activities to ensure full implementation of approved policy.

Comments: Concur. Dallas CMOP Configuration plan was updated January 23, 2022, to ensure the OIG finding is remediated and meets VA regulations. VA OIT requests closure of recommendation 3.

Supporting evidence provided in Appendix A. [The OIG did not include the appendix referenced here as part of this report.]

OIG Recommendation 4: Implement effective configuration control processes that ensure networks devices maintain standards mandated by the VA Office of Information and Technology Configuration Control Board.

Comments: Concur. VA updated the baseline version of the Internetwork Operating System (IOS) to ensure network devices maintain VA OIT Configuration Control Board mandated standards.VA OIT requests closure of recommendation 4. Supporting evidence provided in Appendix A. [The OIG did not include the appendix referenced here as part of this report.].

OIG Recommendation 5: Remove or disable group accounts to comply with established requirements and criteria.

Comments: Concur. Dallas CMOP will work with the Director, Infrastructure Operations Account Management to remediate and correct the accounts in accordance with VA policy. The Dallas CMOP information technology (IT) department is working with Leidos/Pingwind (vendor) to perform an analysis of the effect on the system. The target completion date is July 31, 2022

OIG Recommendation 6: Ensure employees lock devices when they are unattended.

Comments: Concur. The Dallas CMOP IT staff were debriefed January 12, 2022, on always securing and enforcing proper access to all IT areas. The ramification of unauthorized access has been discussed in-depth and physical security checks and training were reinforced. VA OIT requests closure of recommendation 6. Supporting evidence provided in Appendix A. [The OIG did not include the appendix referenced here as part of this report.]

OIG Recommendation 7: Implement database authentication processes that comply with National Institute of Standards and Technology standards and VA security requirements.

Comments: Concur. The Database Team has remediated the password issue and database scans. The POAM was closed on January 12, 2022. VA OIT requests closure of recommendation 7. Supporting evidence provided in Appendix A. [The OIG did not include the appendix referenced here as part of this report.]

OIG Recommendation 8: Implement a process to retain database logs for a period consistent with VA's record retention policy.

Comments: Concur. The Development, Security and Operations (DevSecOps) Platform Support Database Operations is working with DevSecOps Cybersecurity Management Network Security to further address database cybersecurity audit log capture and retention since the time of this audit visit. The current solution is to install the Imperva agents on all database servers. The enterprise database cybersecurity audit logging and retention project is scheduled to be completed by September 2023. Platform Support and Cybersecurity Management Network Security will be targeting the completion of the Dallas CMOP database cybersecurity audit log and retention implementation by the end of August 2022. The target completion date is September 2023.

OIG Recommendation 9: Establish a process for validating and logging the sanitization of hard drives.

Comments: Concur. The Dallas CMOP staff were retrained on the VA media destruction program user guide that outlines the Tucson CMOP media sanitization process to ensure compliance with VA policies. Training was completed and documented on February 7, 2022. VA OIT requests closure of

recommendation 9. Supporting evidence provided in Appendix A. [The OIG did not include the appendix referenced here as part of this report.]

OIG Recommendation 10: Implement parking barriers that meet VA Physical Security & Resiliency Design Manual.

Comments: Concur. OIG assessed the Dallas CMOP outside perimeter for parking barriers and bollards for vehicle attacks. OIG stated that no perimeter or parking barriers were in use during the time the OIG inspection team was on site and referred to the VA Physical Security and Resiliency Design Manual. eMASS is the system VA uses to track ATO documentation. VA is currently using National Institute of Standards and Technology (NIST) publication 800-53a revision 4, which does not require Physical and Environmental (PE) security controls, PE-3 parking barriers and bollards for vehicles attacks. OIG used NIST 800-53a revision 5; the updated version does require the PE security controls, PE-3 parking barriers and bollards for vehicle attacks. Dallas CMOP will work with the Veterans Health Administration to complete a risk assessment of the site and will have a plan in place to fix or accept the risk by December 2022. The target completion date is December 2022.

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 Ginalynn Alvarado Keith Hargrove Jack Henserling Shawn Hill Timothy Moorhead Albert Schmidt Adam Sowells Brandon Zahn
Other Contributors	Charles Hoskinson Chris Dong

Report Distribution

VA Distribution

Office of the Secretary
Veterans Benefits Administration
Veterans Health Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel
Office of Acquisition, Logistics, and Construction
Board of Veterans' Appeals
Director, Dallas Consolidated Mail Order Pharmacy

Non-VA Distribution

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

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