US DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS HEALTH ADMINISTRATION

Inspection of Information Security at the VA El Paso Healthcare System in Texas

Information Security Inspection	23-01179-204	September 27, 2023

BE A

VOICE FOR VETERANS

REPORT WRONGDOING

va.gov/oig/hotline | 800.488.8244

OUR MISSION

To serve veterans and the public by conducting meaningful independent oversight of the Department of Veterans Affairs.

CONNECT WITH US

Subscribe to receive updates on reports, press releases, congressional testimony, and more. Follow us at @VetAffairsOIG.

PRIVACY NOTICE

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

Visit our website to view more publications.
va.gov/oig

Executive Summary

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

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

In 2020, the OIG also started an information security inspection program. These inspections assess whether VA facilities are meeting federal security requirements related to three control areas the OIG determined to be at highest risk.[4] Typically, facilities selected for these inspections either were not included in the annual audit sample or had previously performed poorly. The OIG conducted this inspection to determine whether the VA El Paso Healthcare System in Texas was meeting federal security guidance. The OIG selected the VA El Paso Healthcare System because it had not been previously visited as part of the annual FISMA audit. The inspection scope and methodology are described in appendix C.

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

1. **Configuration management controls** identify and manage security features for all hardware and software components of an information system.[5]
2. **Security management controls** "establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of the procedures."[6]

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

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

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

[4] Effective August 2022, the OIG removed a fourth control area—contingency planning—from its information security inspections because this area is largely enterprise controlled and not a significant risk at the local level. Appendix B presents background information on federal information security requirements.

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

[6] GAO, *FISCAM*.

3. **Access controls** provide reasonable assurance that computer resources are restricted to authorized individuals. Access also includes physical and environmental controls associated with physical security, such as authorization, visitors, monitoring, delivery, and removal.[7]

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

What the Inspection Found

The OIG identified deficiencies in configuration management and access controls.

Two Configuration Management Controls Had Deficiencies

The VA El Paso Healthcare System had deficiencies in two configuration management controls:

- **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.[8]

VA has a vulnerability management program, but it can be improved. Prior FISMA audits repeatedly found deficiencies in VA's vulnerability management. Consistent with those findings, the team found operating systems that were no longer supported by the vendor and applications with missing security patches at the healthcare system. 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, the team found vulnerabilities that OIT did not detect. For example, the OIG found 65 critical vulnerabilities that OIT did not. The inspection team also identified 195 vulnerabilities—96 critical vulnerabilities on 9 percent of the devices and 99 high-risk vulnerabilities on 32 percent of the devices—that were not mitigated within the required 30 or 60 days. While OIT is aware of many of the vulnerabilities, plans of actions and milestones were not created to manage them according to the vulnerability management process.[9] The system used to report vulnerabilities to facilities was not complete and accurate. For example, the system did not have host names for 16 percent of the entries.

[7] GAO, *FISCAM*.

[8] NIST Special Publication 800-53.

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

Despite VA's patch management measures, the inspection team identified several devices missing security patches. For instance, several devices with critical and high-risk vulnerabilities had patches available that were not applied. Without these controls, critical systems may be at unnecessary risk of unauthorized access, alteration, or destruction.

Six Access Controls Had Deficiencies

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

- **Physical access** includes devices and barriers to prevent movement from publicly accessible areas to nonpublic areas.[10]
- **Reviewing physical access logs** can help identify suspicious activity, anomalous events, or potential threats.
- **Video surveillance** is the use of cameras installed at strategic locations and is required for data centers.[11]
- **Environmental controls** maintain and monitor temperature and humidity where communication equipment is located.[12]
- **Water detection** senses the presence of water in the vicinity of information systems.
- **Emergency power shutoff** bypasses power from an uninterruptible power supply.

Restricting physical access protects IT resources from loss or impairment. The OIG discovered multiple communication rooms where physical access was not effectively controlled. The healthcare system had an automated physical access control system in which staff use badges to enter buildings and rooms. However, the system was not fully operational. Instead, employees use keys to gain access. Key inventories, which are required every six months, had not been conducted at the facility because the locksmith relied on individuals to return keys when no longer needed. Facility managers are aware of the deficient physical access control system and plan to replace it.

Physical access logs were not being reviewed as required by OIT policy.[13] The healthcare system uses a centralized system to control physical access to the datacenter and communication rooms. The system also maintains access logs to those rooms. The area manager is required to review access logs on a quarterly basis. Reviewing physical access logs can help identify suspicious

[10] NIST Special Publication 800-53.

[11] Development, Security, and Operations, End User Operations, "Physical and Environmental Protection" (standard operating procedure), March 23, 2022; NIST Special Publication, 800-53.

[12] NIST Special Publication, 800-53.

[13] Development, Security, and Operations, End User Operations, "Physical and Environmental Protection."

activity, anomalous events, or potential threats.[14] The lack of log reviews increases the likelihood that potential threats are not identified resulting in the loss of confidentiality of, integrity of, or access to VA sensitive data.[15]

The inspection team discovered that several surveillance cameras were inoperable at the healthcare system, including cameras that monitor the data center. Facility managers were aware of the deficient surveillance system and said it was no longer supported. Consequently, the healthcare system is in the process of acquiring a contract to upgrade the video surveillance system. Ineffective monitoring of activities supporting information systems minimizes the facility's incident response capabilities in the event of a security compromise. The lack of an effective incident response can undermine management's awareness of security vulnerabilities that could hinder the operation of mission-critical systems.

During walk-throughs, the inspection team discovered several communication rooms without temperature or humidity controls. Temperature extremes can reduce efficiency and lead to other problems, including premature aging and failure of equipment. High humidity can corrode internal components and cause degradation of electrical functions. Insufficient environmental controls can have a significant adverse impact on the availability of systems needed to support the organizational mission and business functions.[16]

According to facility management, the data center water detection sensors were not operational. However, they were in the process of acquiring a replacement system as part of the physical access control system effort. OIT requires facility managers and OIT's area manager to be alerted when automated mechanisms detect the presence of water in the vicinity of the information system. Without functioning water sensors, VA cannot minimize losses or prevent incidents through early leak detection.

The area manager at the El Paso Healthcare System could not provide evidence that the emergency power shutoff for the data center was tested. The emergency power shutoff bypasses power from the uninterruptible power. The standard operating procedure requires the emergency power shutoff to be inspected annually during uninterruptible power supply testing.[17] Routine testing helps ensure that the bypass will function properly during an emergency. This control primarily applies to the safety of personnel. However, it could protect equipment from damage

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

[15] 38 U.S.C. § 5727 defines "VA sensitive data" as "all Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information and includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, and records about individuals requiring protection under applicable confidentiality provisions."

[16] NIST Special Publication 800-53.

[17] Development, Security, and Operations, End User Operations, "Physical and Environmental Protection" (standard operating procedure), March 23, 2022; NIST Special Publication 800-53.

caused by a malfunctioning uninterruptible power supply. Without routine testing, the emergency power shutoff could malfunction during an emergency and could adversely affect the safety of personnel and the integrity and availability of VA sensitive data.

What the OIG Recommended

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

1. Implement a more effective vulnerability management program to address security deficiencies identified during the inspection.
2. Ensure vulnerabilities are remediated within OIT’s established time frames.
3. Ensure that physical access for the data center and communication rooms are reviewed on a quarterly basis.

The OIG also made five recommendations to the VA El Paso Healthcare System director:

4. Ensure physical access controls are implemented for communication rooms.
5. Ensure a video surveillance system is operational and monitored for the data center.
6. Ensure communication rooms with infrastructure equipment have adequate environmental controls.
7. Ensure water detection sensors are installed in the data center.
8. Test the emergency power bypass during annual uninterruptible power supply testing and document results.

VA Comments and OIG Response

The assistant secretary for information and technology and chief information officer concurred with recommendations 1 through 8 and requested that recommendations 1, 2, and 3 be closed due to corrective actions he said were completed. For recommendations 1 through 8, the planned corrective actions are responsive to the intent of the recommendations. The assistant secretary provided evidence to support actions addressing recommendation 3 were completed, and the OIG considers this recommendation closed.

The assistant secretary provided evidence to support remediation actions are in progress for recommendations 1 and 2. The evidence is the result of an enterprise-wide process established after the inspection team reported the remediation deficiency to VA. While this is a first step in addressing the report’s findings with respect to vulnerability remediation, it does not yet demonstrate that the new process is working as intended. The OIG will continue to monitor the remediation of vulnerabilities and the creation of plans of action and milestones for vulnerabilities that cannot be remediated during the information security inspections.

Recommendations 1 and 2 will be closed when VA can demonstrate that the plan of action and milestones process effectively mitigates security risks for unremedied security vulnerabilities.

The OIG will monitor implementation of the planned actions and will close the open recommendations when VA provides evidence demonstrating progress in addressing the issues identified. The full text of the assistant secretary's response is included in appendix D.

Larry M. Reinkemeyer

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations.

Contents

Abbreviations

eMASS	Enterprise Mission Assurance Support System
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
GAO	Government Accountability Office
IT	information technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information and Technology
VHA	Veterans Health Administration

Introduction

Information security controls protect VA systems and data from unauthorized access, use, modification, or destruction. To determine compliance with the Federal Information Security Modernization Act of 2014 (FISMA), the VA Office of Inspector General (OIG) contracts with an independent public accounting firm that conducts an annual audit of VA's information security program and practices.[18] 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.[19] Appendix A provides more details of the most recent FISMA audit.

In 2020, the OIG also started an information security inspection program. These inspections assess whether VA facilities are meeting federal security requirements that protect systems and data from unauthorized access, use, modification, or destruction. They are typically conducted at selected facilities that have not been assessed in the sample for the annual FISMA audit or at facilities that previously performed poorly. Inspections provide recommendations to VA on enhancing information security oversight at local and regional facilities.[20] Appendix C provides more detail on the inspection scope and methodology.

The OIG conducted this inspection to determine whether the VA El Paso Healthcare System in Texas was meeting federal security guidance. The OIG selected the VA El Paso Healthcare System because it had not been previously visited as part of the annual FISMA audit.

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

Security Controls

Both the Office of Management and Budget and NIST provide criteria to evaluate security controls. These criteria provide requirements for establishing, implementing, operating,

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

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

[20] The OIG provided VA with a report 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 report 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.

monitoring, reviewing, maintaining, and improving a documented information security management system.[21]

According to VA Handbook 6500, responsibility for developing and maintaining information security policies, procedures, and control techniques lies with the assistant secretary for information and technology, who also serves as VA's chief information officer. In addition, VA Handbook 6500 describes the risk-based process for selecting system security controls, including the operational requirements.[22] VA established guidance outlining both NIST- and VA-specific requirements to help information system owners select the appropriate controls to secure their systems.

The OIG information security inspections are focused on three security control areas that apply to local facilities and have been selected based on their level of risk, as shown in table 1.[23]

Table 1. Security Controls Evaluated by the OIG

Control area	Purpose	Examples evaluated
Configuration management	Identify and manage security features for all hardware and software components of an information system	Component inventory, baseline configurations, configuration settings, change management, vulnerability management, and flaw remediation
Security management	Establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of the procedures	Risk management, assessment, authorization, and monitoring
Access	Provide reasonable assurance that computer resources are restricted to authorized individuals	Access, identification, authentication, audit, and accountability, including related physical security controls

Source: VA OIG analysis.

Without these critical controls, VA's systems are at risk of unauthorized access or modifications. A cyberattack could destroy, disrupt access to, or allow malicious control of personal information belonging to patients, dependents, beneficiaries, VA employees, contractors, or volunteers.

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

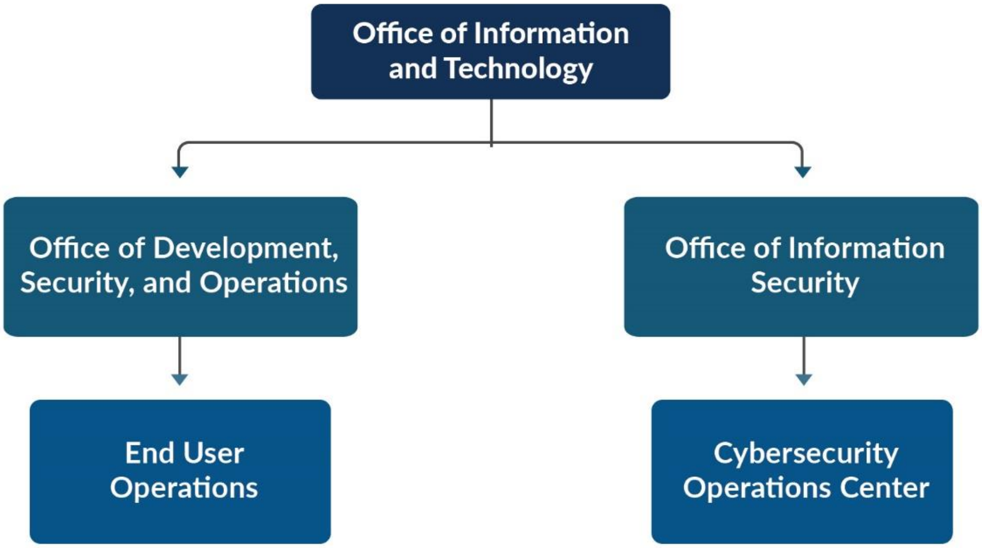
[22] VA Handbook 6500, *Risk Management Framework for VA Information Systems: VA Information Security Program*, February 2021.

[23] Effective August 2022, the OIG removed a fourth control area—contingency planning—from its information security inspections because this area is largely enterprise controlled and not a significant risk at the local level.

Office of Information and Technology Structure and Responsibilities

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

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


Office of Information and Technology

Office of Development, Security, and Operations

Office of Information Security

End User Operations

Cybersecurity Operations Center

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

End User Operations provides onsite and remote support to IT customers across all VA administrations and special program offices, including direct support of approximately 400,000 VA employees and approximately 100,000 contractors who are issued government furnished IT equipment and access. End User Operations provisions computing devices; conducts new facility activations; performs moves, adds, and changes; executes local system implementations; and engages VA's customers across the nation to meet IT support needs. OIT assigns dedicated End User Operations and Office of Information Security personnel to the VA El Paso Healthcare System, including system stewards who are responsible for managing system plans of action and milestones to ensure all assessed and scanned vulnerabilities are documented.

Results of Previous Projects

As previously mentioned, the OIG issues annual reports on VA's information security program. The FISMA audit is conducted in accordance with guidelines issued by the Office of Management and Budget and applicable NIST information security guidelines.[24] The fiscal year 2022 FISMA audit, conducted by independent public accounting firm CliftonLarsonAllen LLP, evaluated 47 major applications and general support systems hosted at 23 VA facilities, including the testing of selected management, technical, and operational controls outlined by NIST.[25] CliftonLarsonAllen LLP made 26 recommendations, listed in appendix A.

All 26 recommendations are repeated from the prior annual audit, indicating that VA continues to face significant challenges in complying with FISMA requirements.[26] Repeat recommendations included addressing deficiencies in configuration management, security management, and access controls.

A statement prepared by the Government Accountability Office (GAO) for a House Veterans' Affairs subcommittee hearing in November 2019 said VA was one of the federal agencies that continued to have a deficient information security program.[27] According to GAO, VA faced several security challenges while securing and modernizing its information systems, including

- effectively implementing information security controls,
- mitigating known vulnerabilities,
- establishing elements of its cybersecurity risk management program,
- identifying critical cybersecurity staffing needs, and
- managing IT supply chain risks.

GAO concluded that "until VA adequately mitigates security control deficiencies, the sensitive data maintained on its systems will remain at increased risk of unauthorized modification and disclosure, and the system will remain at risk of disruption."[28]

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

[25] OMB, "Security of Federal Automated Information Resources," app 3 in OMB Circular A-130. The appendix defines a general support system as an interconnected set of information resources under the same direct management control which share common functionality.

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

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

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

VA El Paso Healthcare System

The VA El Paso Healthcare System provides healthcare services at seven locations serving southwest Texas and southern New Mexico. The healthcare system provides a wide range of health services for veterans, including general medicine, mental health care, pharmacy, and rehabilitation. The healthcare system also provides emergency care, acute inpatient care, and surgical care through an agreement with William Beaumont Army Medical Center. According to VA, the healthcare system served over 247,000 patients in fiscal year 2022.

VA
U.S. Department of Veterans A
VA Outpatient Clinic
El Paso
VA Heart of Texas Healthcare Network

Figure 2. *VA Outpatient Clinic, El Paso.*
Source: VA OIG inspection team, February 14, 2023.

Results and Recommendations

I. Configuration Management Controls

According to the GAO's *Federal Information System Controls Audit Manual* (FISCAM), configuration management involves identifying and managing security features for all hardware, software, and firmware components of an information system at a given point and systematically controlling changes to that configuration during the system's life cycle. Effective configuration management prevents unauthorized changes to information system resources and provides reasonable assurance that systems are configured and operating securely and as intended. The inspection team reviewed and evaluated 12 configuration management controls drawn from NIST criteria for VA-hosted systems at the VA El Paso Healthcare System to determine if they met federal guidance and VA requirements.

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

Finding 1: The VA El Paso Healthcare System Had Deficiencies in Two Configuration Management Controls

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

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

[29] GAO, *FISCAM*.

[30] GAO, *FISCAM*.

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

Vulnerability Management and Flaw Remediation

VA has a vulnerability management program, but it can be improved. Prior FISMA audits repeatedly found deficiencies in VA's vulnerability management controls. Consistent with those findings, the team identified deficient controls at the VA El Paso Healthcare System.[32] Vulnerability management is the process by which OIT identifies, classifies, and reduces weaknesses and is part of assessing and validating risks, as well as monitoring the effectiveness of a security program. The Cybersecurity Operations Center identifies and reports on threats and vulnerabilities, and OIT conducts scans for vulnerabilities both routinely and randomly, or when new vulnerabilities are identified and reported.

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

NIST assigns severity levels to vulnerabilities by using the Common Vulnerability Scoring System, a framework for communicating the characteristics of software vulnerabilities.[34] The scoring system captures the principal characteristics of a vulnerability and produces a numerical score reflecting its severity. Numerical scores are classified as 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-risk vulnerabilities have a score between 9.0 and 10, while high-risk vulnerabilities have a score between 7.0 and 8.9. VA requires critical-risk vulnerabilities be remediated within 30 days and high-risk vulnerabilities be remediated in 60 days.[35]

The inspection team compared OIT-provided network vulnerability scan results from the VA El Paso Healthcare System against its own scans conducted from February 13–17, 2023. The team and OIT used the same vulnerability scanning tools. The team identified 195 vulnerabilities (96 critical-risk vulnerabilities on nine percent of the devices and 99 high-risk vulnerabilities on 32 percent of the devices) that were not mitigated by within the times established by OIT. Moreover, OIT's security scans did not identify 65 critical-risk vulnerabilities the team

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

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

[34] "Vulnerability Metrics," NIST National Vulnerability Database, accessed June 6, 2023, https://nvd.nist.gov/vuln-metrics/cvss; "Common Vulnerability Scoring System ver. 3.14, Specification Document, Revision 1," Forum of Incident Response and Security Teams (FIRST), accessed June 6, 2023, https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf.

[35] Information System Vulnerability Management Plan Version 1.0, March 28, 2022.

detected.[36] Similarly, the prior FISMA audit found that "VA did not have a complete inventory of all vulnerabilities present on locally hosted systems."[37] The OIG identified critical and high-risk vulnerabilities on 41 percent of the devices at the VA El Paso Healthcare System. Most of the critical and high-risk vulnerabilities were found on devices not hosted in medical device and special purpose system network segments. While OIT is aware of many of the vulnerabilities, its vulnerability management process was not followed. This led to plans of action and milestones not being created for specific vulnerabilities, which would list strategies for remediation or any resource constraints.[38] Without an effective patch management program, vulnerabilities such as security and functionality problems in software and firmware might not be mitigated, increasing opportunities for exploitation.

VA uses its Information Central Analytics and Metrics Platform to report vulnerabilities to facilities for remediation. The OIG found that the information within the platform was not complete and accurate. For example, the February 2023 report contained 15,556 entries for critical-, high-, and medium-risk host vulnerabilities. However, the inspection team found that 2,538 or 16 percent of the entries did not include a host name, as they did not have an appropriate domain name system entry.[39] Not having complete and accurate information in the vulnerability reports can make it difficult for the healthcare system to identify vulnerable devices for remediation. However, according to VA, OIT does use other standard network administration tools to identify devices. Further, inaccurate information may undermine managers' abilities to take appropriate corrective actions.

The healthcare system did not remediate all flaws affecting devices in its network. For example, the inspection team identified vulnerabilities, such as operating systems that were no longer supported by the vendor and applications with missing security patches. The flaw remediation process identifies, reports, and corrects system flaws, including installing security-relevant software and firmware updates.[40] Security-relevant updates include patches, service packs, and malicious code signatures. Security patches are usually the most effective way to mitigate

[36] The difference in scan results can be attributed to multiple factors. First, the scans are conducted at different points in time, so devices could have been added to or removed from the network between scans. Second, the OIG uses all available plug-ins with its vulnerability scanner, while OIT does not. According to OIT, they do not use all plug-ins because of potential impact on medical devices. Finally, the scans are conducted from different places in the network, which could be impacted by access controls.

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

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

[39] A host name is the name of a device that the network associates to a given IP address.

[40] NIST Special Publication 800-53.

software flaw vulnerabilities. According to GAO, a patch is a piece of software code inserted into a program to temporarily fix a defect until an updated software version is released. NIST further explains that patches correct security and functionality problems in software and firmware. Patch management is how OIT acquires, tests, applies, and monitors updates that address security and functionality problems. Patch management is a critical process used to help alleviate many of the challenges in securing systems from cyberattack. Previous FISMA audits have repeatedly found deficiencies in this area.[41]

Finding 1 Conclusion

The VA El Paso Healthcare System's vulnerability management controls did not identify all network weaknesses, such as unsupported versions of applications, and flaw remediation controls did not ensure comprehensive patch management. Further, vulnerabilities were not always remediated within times established by OIT. Without effective configuration management controls, management does not have adequate assurance that the system and network will perform as intended and to the extent needed to support VA's mission.

Recommendations 1–2

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

1. Implement a more effective vulnerability management program to address security deficiencies identified during the inspection.
2. Ensure vulnerabilities are remediated within OIT's established time frames.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 1 and 2. The assistant secretary reported that the corrective actions were completed and requested the recommendations be closed.

In addressing recommendation 1, the assistant secretary reported that VA had developed an enterprise-wide process to link vulnerabilities to plan of action and milestones items and provided documentation indicating that the OIG- and VA-identified vulnerabilities had either been remediated or have a plan of action and milestones established for remediation. In addressing recommendation 2, the assistant secretary reported that the root causes for

[41] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2022*, Report No. 22-01576-72, May 17, 2023; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2021*, Report No. 21-01309-74, April 13, 2022; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2020*, Report No. 20-01927-104, April 29, 2021.

recommendations 1 and 2 were the same, and therefore actions taken to address recommendation 1 also address recommendation 2.

OIG Response

The assistant secretary for information and technology and chief information officer submitted a responsive action plan for recommendations 1 and 2. Further, the assistant secretary provided evidence to support actions addressing recommendations 1 and 2 are in progress. However, this evidence is the result of an enterprise-wide process established after the inspection team reported the remediation deficiency to VA. While this is a first step in addressing the report's findings with respect to vulnerability remediation, it does not yet demonstrate that the new process is working as intended. The OIG will continue to monitor the remediation of vulnerabilities and the creation of plans of action and milestones for vulnerabilities that cannot be remediated during the information security inspections. Recommendations 1 and 2 will be closed when VA can demonstrate that the plan of action and milestone process effectively mitigates security risks for unremedied security vulnerabilities. The full text of the assistant secretary's response is included in appendix D.

II. Security Management Controls

According to FISCAM, security management controls establish a framework and continuous cycle for assessing risk, developing security procedures, and monitoring the effectiveness of the procedures. The inspection team evaluated five security management critical elements: establish a security management program, assess and validate risk, document and implement security control policies and procedures, monitor the effectiveness of the security program, and effectively remediate information security weaknesses.[42]

Finding 2: The VA El Paso Healthcare System Had No Security Management Deficiencies

To assess security controls, the inspection team reviewed local security management policies, standard operating procedures, and applicable VA policies. These included documentation from the Enterprise Mission Assurance Support Service (eMASS), VA's cybersecurity management service for workflow automation and continuous monitoring. Among the topics reviewed were the system security plan, security authorization and risk assessment, security control policies and procedures, and plans of action and milestones for known deficiencies. The team also interviewed the area manager, information system security officer, and facility manager. Finally, the team conducted walk-throughs of the facility.

The OIG found that the VA El Paso Healthcare System has a system security plan and risk assessment that has been documented and approved by management. There are documented security control policies and procedures in place that are signed and approved. The VA El Paso Healthcare System has developed and implemented plans of action and milestones for self-identified weaknesses. The plans of action and milestones have been periodically reviewed.

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

III. Access Controls

Previous FISMA reports have repeatedly identified access controls as a nationwide issue for VA. Access controls can be both logical and physical and provide reasonable assurance that computer resources are restricted to authorized individuals. Logical access controls require users to authenticate themselves and limit the resources they can access and restricts actions they can take. Physical access controls involve restricting physical access to computer resources and protecting them from loss or impairment. At the VA El Paso Healthcare System, the inspection team reviewed three critical access control elements, each of which contain multiple controls.[43]

Finding 3: The El Paso VA Healthcare System Had Deficiencies in Six Access Controls

To evaluate the VA El Paso Healthcare System's access controls, the inspection team interviewed the area manager, information system security officer, biomedical equipment supervisor, database administrators, and local IT specialists; reviewed local policies and procedures; and conducted walk-throughs of the facility.[44]

The OIG found the following issues with access controls at the VA El Paso Healthcare System:

- Physical access was not effectively controlled.
- Physical access logs were not reviewed.
- Video surveillance for the data center was not operational.
- Several communication rooms containing infrastructure network equipment lacked environmental controls.
- Water detection sensors were not operational in the data center.
- Emergency power shutoff had not been tested.

Physical Access

Restricting physical access helps protect IT resources from loss or impairment. The OIG discovered multiple communications rooms where physical access was not effectively controlled. Physical access includes devices and barriers to prevent movement from publicly accessible areas to nonpublic areas.[45] The healthcare system had an automated physical access control system in which a badge is used to gain entry to buildings and rooms. However, the system was not fully operational. Instead, employees use keys to gain access. A key inventory is

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

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

[45] NIST Special Publication 800-53.

required every six months, but an inventory was not conducted at the facility because the locksmith relies on individuals to return keys when they are no longer needed. The facility is aware of the issues with the physical access control system and plans to replace it.

Monitoring Physical Access

The OIG discovered that the physical access logs were not reviewed as required by OIT policy.[46] The VA El Paso Healthcare System uses a centralized system to control physical access to the data center and communication rooms. The system also maintains access logs to those rooms. The area manager is required to review access logs on a quarterly basis. Reviewing physical access logs can help identify suspicious activity, anomalous events, or potential threats.[47] The lack of log reviews increases the likelihood that potential threats are not identified resulting in the loss of confidentiality of, integrity of, or access to VA sensitive data.[48]

Video Surveillance

During the facility walk-through, the inspection team discovered that several cameras were inoperable at the VA El Paso Healthcare System, including in the data center. Video surveillance is the use of cameras installed at strategic locations and is required for data centers.[49] Managers were aware of the deficient surveillance system and said it was no longer supported by the vendor. Consequently, the healthcare system is in the process of acquiring a contract to upgrade the video surveillance system throughout the facility. Ineffective monitoring of activities supporting information systems minimizes the facility's incident response capabilities in the event of a security compromise. The lack of an effective incident response can undermine management's awareness of security vulnerabilities that could hinder the operation of mission-critical systems.

Temperature and Humidity Controls

During walk-throughs, the inspection team discovered several communication rooms without temperature or humidity controls. Environmental controls maintain and monitor temperature and

[46] Development, Security, and Operations, End User Operations, "Physical and Environmental Protection."

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

[48] 38 U.S.C. § 5727 defines "VA sensitive data" as "all Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information and includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, and records about individuals requiring protection under applicable confidentiality provisions."

[49] Development, Security, and Operations, End User Operations, "Physical and Environmental Protection"; NIST Special Publication 800-53.

humidity where communication equipment is located.[50] Equipment was installed in communication rooms without sufficient environmental controls. Temperature extremes can cause reduced efficiency and a variety of problems, including premature aging and failure of equipment. High humidity can cause corrosion of internal components and degradation of electrical functionality. This is a risk because insufficient environmental controls can have a significant adverse impact on the availability of systems that are needed to support the organizational mission and business functions.

Water Detection

Water sensors detect the presence of water in a data center and can help minimize damage to equipment due to water leaks. OIT requires facility management and OIT's area manager to be alerted when automated mechanisms detect the presence of water in the vicinity of information systems. According to facility management, the data center water detection sensors were not operational. However, they were in the process of acquiring a replacement system as part of the physical access control system effort. Without functioning water sensors, VA cannot minimize losses or prevent incidents through early leak detection.

Emergency Power Shutoff

The area manager at the El Paso Healthcare System could not provide evidence that the emergency power shutoff for the data center was tested as required by policy. The emergency power shutoff bypasses power from the uninterruptible power supply and is primarily applied to facilities that contain concentrations of system resources, including data centers, mainframe computer rooms, server rooms, and areas with computer-controlled machinery. The standard operating procedure requires the emergency power shutoff to be inspected annually during uninterruptible power supply testing.[51] Routine testing helps ensure that the bypass will function properly during an emergency. This control primarily applies to the safety of personnel. However, it could protect equipment from damage caused by a malfunctioning uninterruptible power supply. Without routine testing, the emergency power shutoff could malfunction during an emergency and could adversely impact the safety of personnel and the integrity and availability of VA sensitive data.

Finding 3 Conclusion

The VA El Paso Healthcare System did not control physical access, neither through its control system nor key management. The area manager is not reviewing physical access to the data center or communication rooms. Additionally, the data center video surveillance was inoperable.

[50] NIST Special Publication 800-53.

[51] Development, Security, and Operations, End User Operations, "Physical and Environmental Protection" (standard operating procedure), March 23, 2022; NIST Special Publication 800-53.

Furthermore, several communication rooms did not have temperature or humidity controls, which could have a significant adverse impact on the availability of systems. Water detection sensors, which could diminish or prevent damage caused by leaks, were not operational in the data center. Finally, the emergency power shutoff was not tested as required. Unless the healthcare system takes corrective actions, it risks unauthorized access to critical network resources, inability to respond effectively to incidents, and loss of personally identifiable information.

Recommendations 3–8

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

3. Ensure that physical access for the data center and communication rooms are reviewed on a quarterly basis.

The OIG made the following recommendations to the VA El Paso Healthcare System director:

4. Ensure physical access controls are implemented for communication rooms.
5. Ensure a video surveillance system is operational and monitored for the data center.
6. Ensure communication rooms with infrastructure equipment have adequate environmental controls.
7. Ensure water detection sensors are implemented in the data center.
8. Test the emergency power bypass during annual uninterruptible power supply testing and document results.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 3 through 8. The assistant secretary reported that corrective actions were completed and requested recommendation 3 be closed.

To address recommendation 3, the assistant secretary provided evidence showing that monthly reports of access to the OIT areas are reviewed. For recommendation 4, the assistant secretary indicated that VA developed a detailed plan to upgrade physical access controls system for communication rooms and that the VA Police Services security system will also be upgraded. Regarding recommendation 5, the assistant secretary stated that VA developed a detailed plan to upgrade all cameras that will be monitored continuously as required. For recommendation 6, the assistant secretary stated that Facility Support Services will work with OIT to verify temperature sensor needs and install devices as appropriate. However, he indicated that VA determined it would not be fiscally responsible to deploy the required infrastructure for full remediation at this time since a new facility is set to activate in FY 2028. For recommendation 7, the assistant secretary said VA awarded a contract that included a requirement to design appropriate water sensors. To address recommendation 8, the assistant secretary indicated that prior to testing emergency bypass power, Facility Support Services will acquire spare parts to be maintained on hand to repair any damage incurred from testing.

OIG Response

OIT's corrective action plans are responsive to the intent of the recommendations. The assistant secretary provided evidence to support actions addressing recommendation 3 were completed, and the OIG considers this recommendation closed. The OIG will monitor implementation of the planned actions and will close recommendations 4 through 8 when VA provides evidence demonstrating progress in addressing the issues identified.

Appendix A: FISMA Audit for FY 2022 Report Recommendations

In the FISMA audit for FY 2022, CliftonLarsonAllen LLP made 26 recommendations. Of these, all 26 were repeat recommendations from the prior year. The FISMA audit assesses the agencywide security management program, and recommendations in the FISMA report are not specific to the El Paso Healthcare System. 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 documentation including control assessments on risk-based rotation as needed. Such updates will ensure all required information is included and accurately reflects the current environment.
6. Implement improved processes to ensure compliance with VA password policy and security standards on domain controls, operating systems, databases, applications, and network devices.
7. Implement periodic reviews to minimize access by system users with incompatible roles, permissions in excess of required functional responsibilities, and unauthorized accounts.
8. Enable system audit logs on all critical systems and platforms and conduct centralized reviews of security violations across the enterprise.
9. Implement improved processes for establishing and maintaining accurate data within VA systems used for background investigations.
10. Strengthen processes to ensure appropriate levels of background investigations are completed for applicable VA employees and contractors.

11. Implement more effective automated mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and web application servers.
12. Implement a more effective patch and vulnerability management program to address security deficiencies identified during our assessments of VA's web applications, database platforms, network infrastructure, and workstations.
13. Maintain a complete and accurate security baseline configuration for all platforms and ensure all baselines are appropriately monitored for compliance with established VA security standards.
14. Implement improved network access controls that restrict medical devices from systems hosted on the general network.
15. Enhance procedures for tracking security responsibilities for networks, devices, and components not managed by the Office of Information and Technology to ensure vulnerabilities are remediated in a timely manner.
16. Implement improved processes to ensure that all devices and platforms are evaluated using credentialed vulnerability assessments.
17. Implement improved procedures to enforce standardized system development and change control processes that integrates information security throughout the life cycle of each system.
18. Review system boundaries, recovery priorities, system components, and system interdependencies and implement appropriate mechanisms to ensure that established system recovery objectives can be measured and met.
19. Ensure that contingency plans for all systems are updated to include critical inventory components and are tested in accordance with VA requirements.
20. Implement more effective agencywide incident response procedures to ensure timely notification, reporting, updating, and resolution of computer security incidents in accordance with VA standards.
21. Ensure that systems and applications are adequately and monitored to facilitate agencywide awareness of information security events.
22. Implement improved safeguards to identify and prevent unauthorized vulnerability scans on VA networks.
23. Implement improved measures to ensure that all security controls are assessed in accordance with VA policy and that identified issues or weaknesses are adequately documented and tracked within Plans of Action and Milestones.

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

Appendix B: Background

Federal Information System Controls Audit Manual

The 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 naming and describing physical and functional characteristics of a controlled item, as well as performing activities to define, track, store, manage, and retrieve configuration items. Examples of these controls are baseline configurations, configuration settings, and component inventories.

- **Authorize, test, approve, and track changes** by formally establishing a change management process, with management's authorization and approval of the changes. This element includes documenting and approving test plans, comprehensive and appropriate testing of changes, and creating an audit trail to clearly document and track changes.

- **Conduct routine configuration monitoring** to determine the accuracy of the changes that should address baseline and operational configuration of hardware, software, and firmware.[52] Products should comply with applicable standards and the vendors' good security practices. The organization should have the ability to monitor and test to determine if a system is functioning as intended, as well as to determine if networks are appropriately configured and paths are protected between information systems.

- **Update software on a timely basis** by scanning software and updating it frequently to guard against known vulnerabilities. In addition, security software should be kept current by establishing effective programs for patch management, virus protection, and identification of other emerging threats. Software releases should be controlled to prevent the use of noncurrent software. Examples of these controls are software usage

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

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

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

FISCAM has seven critical elements for security management:

- **Institute a security management program** that establishes policies, plans, and procedures clearly describing all major systems and facilities and that outlines the duties of those responsible for overseeing security as well as those who own, use, or rely on the organization’s computer resources. There should be a clear security management structure for systems and devices as well as for business processes. Examples of specific controls are system security plans, plan updates, activity planning, and resource allocation.
- **Assess and validate risk** by comprehensively identifying and considering all threats and vulnerabilities. This step ensures that agencies address the greatest risks and appropriately decide to accept or mitigate risks. Examples of these controls are security certification, accreditation, categorization, and risk assessment.
- **Document and implement security control policies and procedures** that appropriately address general and application controls and ensure users can be held accountable for their actions. These controls, which are more general at the entity wide level and more specific at the system level, should be approved by 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.[53]

FISCAM lists six access control critical elements:

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

[53] GAO, *FISCAM*.

Federal Information Security Modernization Act of 2014

The 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.[54]

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

NIST Information Security Guidelines

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

[54] FISMA.

Appendix C: Scope and Methodology

Scope

The inspection team conducted its work from January 2023 through July 2023. The team evaluated configuration management, 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 VA El Paso Healthcare System IT security and operations, and privacy compliance. The team conducted vulnerability and configuration testing to determine local systems' security compliance. Finally, the team analyzed the results of testing, interviews, and the inspection to identify policy violations and threats to security.

Internal Controls

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

Data Reliability

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

In addition, computer-processed data included vulnerabilities provided by the cybersecurity operation center. The team used this data to compare vulnerabilities identified by VA with those identified by the OIG. To test for reliability, the team determined whether any data were missing from key fields or were outside the times requested. The review team also assessed whether the data contained obvious duplication of records, alphabetic or numeric characters in incorrect fields, or illogical relationships among data elements. Testing of the data disclosed that they were sufficiently reliable for the review objectives.

Government Standards

The OIG conducted this 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: August 21, 2023

From: Assistant Secretary for Information and Technology and Chief Information

Officer (005)

Subj: Office of Inspector General Draft Report: Inspection of Information Security at the VA El Paso Healthcare System in Texas (VIEWS 10631094)

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

1. Thank you for the opportunity to review the Office of Inspector General (OIG) draft report, Inspection of Information Security at the VA El Paso Healthcare System in Texas (Project Number 2023-01179-AE-0043).

2. The Office of Information and Technology (OIT) submits the attached written comments.

The OIG removed point of contact information prior to publication.

(Original signed by)

Kurt D. DelBene

Attachment

Attachment

Office of Information and Technology
Comments on Office of Inspector General Draft Report,
Inspection of Information Technology Security at the El Paso Healthcare System, Project Number 2023-01179-AE-0043
(VIEWS 10631094)

Recommendation 1: Implement a more effective vulnerability management program to address security deficiencies identified during the inspection.

Comments: Concur.

The Department of Veterans Affairs (VA) Office of Information and Technology (OIT) concurs with Recommendation 1 and requests closure. VA had already developed, and was implementing, an enterprise-wide process to link vulnerabilities to Plan of Action and Milestones (POAM) items. However, at the time of the Office of Inspector General's (OIG) inspection, VA had not yet fully implemented this process for all the area boundaries, including the El Paso VA Healthcare System. VA completed this milestone on July 30, 2023. The El Paso VA Healthcare System has now completed the implementation of POAM Vulnerability Portal (PVP)-to-POAM item linkage, as is evidenced in the data export provided in support of VA's request to close this recommendation.

Expected Completion Date: Completed.

VA OIT requests closure of Recommendation 1.

Recommendation 2: Ensure vulnerabilities are remediated within OIT's established time frames.

Comments: Concur.

VA identified the root cause of this recommendation as the same as Recommendation 1. VA remediated the vulnerabilities identified by OIG or added them to POAM items.

VA OIT consistently maintains an enterprise-wide management rate of 90% or greater for critical vulnerabilities. VA's overall compliance percentages provide evidence that VA has implemented, and is managing, an effective vulnerability management program aligned with industry standards. All vulnerabilities fall within the timelines of risk awareness and provide mitigation strategies, explain causes of the extended timelines, and consider the impact of each vulnerability and its remediation on the system.

VA OIT continuously manages vulnerabilities through remediation actions and identifies vulnerabilities by tracking visibility and mitigation efforts. Mitigation actions are recorded and tracked. VA OIT continues to conduct scheduled, regular vulnerability scans per established VA policies and procedures.

Expected Completion Date: Completed.

VA OIT requests closure of Recommendation 2.

Recommendation 3: Ensure that physical access for the data center and communication rooms are reviewed on a quarterly basis.

Comments: Concur.

The Physical Security Section has begun running monthly reports of the access logs and submitting the logs to the OIT chief for review. The access logs include all OIT areas in all facilities. This process will continue until installation of the new access system.

Expected Completion Date: Completed.

VA OIT requests closure of Recommendation 3.

Recommendation 4: Ensure physical access controls are implemented for communication rooms.

Comments: Concur.

VA developed a detailed plan to upgrade the physical access controls system for communication rooms. The VA Police Services security system will also be upgraded during this process.

Expected Completion Date: January 1, 2024.

Recommendation 5: Ensure a video surveillance system is operational and monitored for the data center.

Comments: Concur.

VA developed a detailed plan to upgrade all cameras that will be monitored 24/7 as required. The VA Police Services security systems will also be upgraded to support this requirement.

Expected Completion Date: January 1, 2024.

Recommendation 6: Ensure communication rooms with infrastructure equipment have adequate environmental controls.

Comments: Concur.

Facility Support Services (FSS) will work with OIT to verify temperature sensor needs and install devices as appropriate. FSS will complete the installation of temperature monitors by October 1, 2023.

The facility will conduct a facilities conditions assessment; the facility is currently determining if remediation would be cost-effective. However, to fully remediate the weakness would require revamping the facility infrastructure. Considering that a new health care facility is set to activate in fiscal year 2028, VA determined that it would not be fiscally responsible or in the best interest of the government or taxpayers to deploy the required infrastructure for full remediation at this time.

Expected Completion Date: September 30, 2028.

Recommendation 7: Ensure water detection sensors are implemented in the data center.

Comments: Concur.

In fiscal year 2022, the contracting office and FSS worked to award a contract and assign a task order and purchase obligation. The contract included the requirement to design appropriate water sensors. On May 8, 2023, the design package was approved for award of a construction contract for fiscal year 2024.

Expected Completion Date: April 1, 2024.

Recommendation 8: Test the emergency power bypass during annual uninterruptible power supply testing and document results.

Comments: Concur.

Due to the age of the system and the availability of the componentry, FSS is identifying component spares that will be kept in-house to quickly repair any damage incurred from testing. Once FSS identifies the required spare parts, they will locate the manufacturers/suppliers of these parts to determine cost and availability. The next phase will be to acquire the spares to be maintained on hand.

Expected Completion Date: March 1, 2024.

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

OIG Contact and Staff Acknowledgments

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

Report Distribution

VA Distribution

Office of the Secretary
Veterans Benefits Administration
Veterans Health Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel
Office of Acquisition, Logistics, and Construction
Board of Veterans' Appeals
Director, El Paso VA Healthcare System

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Accountability
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget
US Senate
New Mexico: Martin Heinrich, Ben Ray Lujan
Texas: John Cornyn, Ted Cruz
US House of Representatives
New Mexico: Gabe Vasquez
Texas: Tony Gonzalez

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