DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS HEALTH ADMINISTRATION

Inspection of Information Technology Security at the Harlingen VA Health Care Center in Texas

INFORMATION TECHNOLOGY INSPECTION | REPORT 22-00973-215 | SEPTEMBER 27, 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, and 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 2021 FISMA audit indicated that VA continues to face significant challenges meeting the law's requirements. The audit made 26 recommendations to VA. All 26 recommendations are repeated from the prior annual audit. These 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.[4] They are 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 Harlingen VA Health Care Center in Texas was meeting federal security guidance. The OIG selected the Harlingen center 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.

The OIG's inspection focused on four security control areas that apply to local facilities and have been selected based on their levels of risk:

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

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

[2] NIST *Security and Privacy Controls for Federal Information Systems and Organizations*, 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 2021*, Report No. 21-01309-74, April 13, 2022.

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

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

for recovery of critical operations should interruptions occur.[6] They include 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. They include authorizing and controlling information system components entering and exiting the center and keeping records of those items.[8]

What the Inspection Found

The OIG identified deficiencies with three of the four security control areas: configuration management, contingency planning, and access controls. The inspection team did not identify deficiencies with security management.[9]

Three Configuration Management Controls Had Deficiencies

The Harlingen VA Health Care Center 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 and corrects software defects and often includes system updates, such as security patches.[10]
- **System life cycle** is the process of initiating, developing, implementing, maintaining, and replacing or disposing of systems.[11]

The center did not have accurate listings of information systems' hardware in VA's Enterprise Mission Assurance Support Service, despite OIT and VA's use of automated inventories of its

[6] GAO, *FISCAM*.

[7] GAO, *FISCAM*.

[8] NIST Special Publication 800-53.

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

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

[11] GAO, *FISCAM.*

systems.[12] A complete, accurate, and up-to-date inventory is required to implement an effective security program. Inaccurate component inventories render vulnerability management ineffective.

The OIG determined that OIT's vulnerability identification process and scans were effective; however, the process to remediate identified vulnerabilities needs improvement. OIT scans for vulnerabilities routinely, randomly, and when new vulnerabilities are identified and reported. The inspection team and OIT used the same vulnerability-scanning tools. The inspection team identified 16 vulnerabilities—five critical vulnerabilities on less than 1 percent of the computers, which also had unsupported operating systems, and 11 high-risk vulnerabilities on 20 percent of the computers—that were previously identified by OIT but were not mitigated within OIT's established time frames. VA requires that critical vulnerabilities be remediated within 30 days and high-risk vulnerabilities be remediated in 60 days. The oldest vulnerability was identified on the network in 2013. The OIG found one critical vulnerability on about 1 percent of computers and six high-risk vulnerabilities on 32 percent of the computers that were detectible but not included in prior OIT scan results.[13]

Despite VA's significant patch management measures, the OIG inspection team identified several devices that were missing available patches. Some of these vulnerabilities had been on the network for as long as nine years after initial discovery by VA. Without patches, VA may be placing critical systems at unnecessary risk of unauthorized access, alteration, or destruction.

Over half of the center's network switches used operating systems past their vendor support dates, meaning they would not receive maintenance or vulnerability support. Furthermore, the deficient devices did not meet VA baseline configurations. These devices should have been refreshed to vendor-supported systems before the vendor terminated 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 baseline configurations for network equipment are mandated by the VA OIT Configuration Control Board.

One Contingency Planning Control Was Deficient

The Harlingen VA Health Care Center had security deficiencies in one contingency planning control: system reconstitution, which is the process by which organizations return systems to a fully operational state.

[12] The Enterprise Mission Assurance Support Service is the system VA uses to manage security and privacy risk assessment and system authorization activities. It allows for FISMA systems inventory tracking and reporting activities.

[13] The vulnerabilities had earlier publication dates, which indicated when the scanning software was first able to detect them.

Although the center relied on OIT to continue mission-critical operations in the event of a disaster, the center's plans did not cover the restoration of all local IT operations after a disaster. Local systems not covered include a system used to restrict physical access to sensitive areas and a silent alarm system that alerts police of emergency situations.

Consequently, the center may not have been able to readily recover all operations as they existed before the disaster. After the inspection team reported this finding to the agency, the Texas Valley Coastal Bend Healthcare System updated the contingency plan to address system reconstitution. Accordingly, the OIG made no recommendation for improvement.

Three Access Controls Had Deficiencies

The Harlingen VA Health Care Center had security deficiencies in the following access controls:

- **Audit and monitoring** involve the collection, review, and analysis of events for indications of inappropriate or unusual activity. These controls should be routinely used to assess the effectiveness of other security controls, recognize an attack, and investigate during or after an attack.
- **Fire protection** is the process of employing and maintaining fire detection and suppression systems.
- **Physical access** involves restricting access to computer resources and protecting them from intentional or unintentional loss or impairment.[14]

The inspection team identified deficiencies in logging administrative actions, retaining logs, and reviewing logs for databases at the center. For instance, database event logs of administrative access were overwritten within minutes, in violation of VA policy. The center 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. Without this information, an investigation may be limited or unsuccessful in determining the unauthorized use or modification of center information.

The inspection team found that the center did not have fire detection systems in its two computer rooms and five communication closets. Without these systems, the center may not be able to readily respond to a fire before the activation of sprinkler systems. This could damage organizational assets and result in financial loss or harm to veterans.

The inspection team also noted that one of the computer rooms did not use a visitor access log. As a result, the information security officer and system owner could not verify that appropriate physical security measures were implemented and functioning as intended. Without visitor

[14] NIST Special Publication 800-128; VA Handbook 6500.

access logs, there is no record of visitors who enter the computer room. Consequently, research would be impeded in the event of intentional or unintentional damage to equipment or the room. Center officials implemented visitor access logs in the computer rooms after the OIG brought this issue to their attention.

What the OIG Recommended

The OIG recommended that the assistant secretary for information and technology and chief information officer implement (1) a more effective process to maintain consistent inventory information for all network segments, (2) a vulnerability management program that ensures system changes occur within organization timelines, (3) an effective system life-cycle process to ensure network devices meet standards mandated by the VA OIT Configuration Control Board, and (4) a process to retain database logs for a period consistent with VA's record retention policy. The OIG made these recommendations to the assistant secretary because they are related to enterprise-wide IT security issues similar to those identified during previous FISMA audits and IT security reviews. The OIG also recommended that the Harlingen VA Health Care Center director (5) validate that appropriate physical and environmental security measures are implemented and functioning as intended.[15]

VA Comments and OIG Response

The assistant secretary for information and technology and chief information officer concurred with recommendations 1 through 4 and requested that recommendations 1, 2, and 4 be closed due to corrective actions he said were completed.[16] For recommendations 1, 3, and 4, the planned corrective actions are responsive to the intent of the recommendations. Although the assistant secretary requested closure of recommendation 1, the target date for corrective actions to be completed enterprise-wide is not until November 30, 2022; therefore, the recommendation will remain open. The OIG will monitor implementation of the planned actions related to recommendations 1 and 3 and will close the recommendations when VA provides evidence of addressing the issues identified. Based on evidence provided, the OIG considers recommendation 4 closed.

Regarding recommendation 2, OIT provided reports that indicate the agency is remediating a high percentage of vulnerabilities; however, the agency is still facing challenges with remediating vulnerabilities within established time frames. The inspection team compared the critical vulnerabilities that were identified on the agency's January 2022 and August 2022 vulnerability scans. The comparison indicated that none of the January vulnerabilities were

[15] The recommendation addressed to the director of the healthcare center is directed to anyone in an acting status or performing the delegable duties of the position.

[16] Appendixes D and E contain the full text of the response from the assistant secretary and acting healthcare center director.

remediated by August 2022. Further, the number of critical vulnerabilities in August 2022 that were not remediated within the established time frames increased to 25 critical vulnerabilities from five critical vulnerabilities on certain computers. Consequently, VA needs to develop reports that will highlight older vulnerabilities not remediated within the established time frames. The OIG will monitor implementation of the corrective actions and will close recommendation 2 when VA provides evidence of addressing the issues identified.

The Harlingen VA Health Care Center acting director concurred with recommendation 5. For recommendation 5, 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 of addressing the issue identified.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluation

Contents

Abbreviations

eMASS	Enterprise Mission Assurance Support Services
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Modernization Act
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 Harlingen VA Health Care Center was meeting federal security requirements and complying with related guidance.[17] The inspection team selected the Harlingen center 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.[18] The law requires VA to develop, document, and implement an agencywide information security and risk management program. FISMA also requires chief information officers and other senior agency officials to report annually on the effectiveness of the agency's information security program. In addition, FISMA requires inspectors general 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 IT controls that protect VA systems and data from unauthorized access, use, modification, and destruction. Inspections provide recommendations to VA on enhancing information security oversight at local and regional facilities.[19] The OIG IT inspections review sites not evaluated under the annual FISMA audits, which only inspect a sample or inspect 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 levels of risk, as shown in table 1.

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

[18] FISMA.

[19] 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, and vulnerability management
Contingency planning	Provide reasonable assurance that information resources are protected and the risk of unplanned interruptions is minimized, and 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: VA OIG analysis.

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.[20]

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

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

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

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), depicted in figure 1. 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. OIT's Office of Development, Security, and Operations unifies software development, software operations, service management, information assurance, cybersecurity compliance, performance monitoring, and technical integration. Under this office is End User Operations, which provides onsite and remote support to IT customers across all VA administrations and special program offices, including direct support to VA employees and contractors who are issued government-furnished IT equipment and access. End User Operations provisions computing devices; conducts new facility activations; and executes local system implementations. OIT assigns dedicated End User Operations personnel to Harlingen VA Health Care Center. The Cybersecurity Operations Center—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.

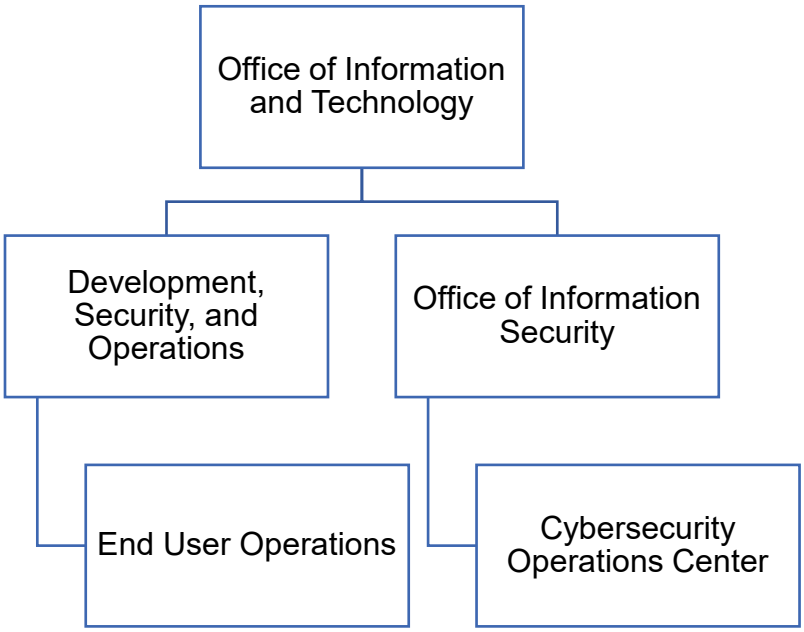

Figure 1. *Organizational structure of OIT entities relevant to this inspection.*
Source: VA OIG analysis.

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 NIST information security guidelines.[22] The fiscal year 2021 FISMA audit, conducted by CliftonLarsonAllen LLP, an independent public accounting firm, assessed VA's information security program through inquiries, observations, and tests of selected controls supporting 50 major applications and general support systems at 24 VA facilities and on the VA Enterprise Cloud, including the testing of selected management, technical, and operational controls outlined by NIST.[23] 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.[24] These recommendations included addressing deficiencies in configuration management, contingency planning, security management, and access controls.

In November 2019 testimony, the Government Accountability Office (GAO) reported that VA was one of the federal agencies that continued to have a deficient information security program.[25] According to the GAO, VA faced several security challenges as it secured and modernized 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.

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

[23] Office of Management and Budget, Circular A-130, app. III, "Security of Federal Automated Information Resources," November 28, 2000. A general support system is "an interconnected set of information resources under the same direct management control that share common functionality."

[24] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2020*, Report No. 20-01927-104, April 29, 2021; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2021*, Report No. 21-01309-74, April 13, 2022. Appendix B presents information about FISMA and other federal criteria and standards discussed in this report.

[25] 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."[26]

Harlingen VA Health Care Center

The Harlingen center is part of the Texas Valley Coastal Bend Healthcare System (figure 2). The system completes about 300,000 outpatient visits each year. It operates a 100-patient home-based primary care program and a 200-patient care coordination home telehealth program. By using two inpatient and emergency department contracts with local medical centers, the system provides approximately 1,600 hospital admissions and 1,200 emergency room visits every year.

Figure 2. *Harlingen VA Health Care Center.*
Source: VA OIG inspection team, January 14, 2022.

[26] 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 Harlingen VA Health Care Center. Of the four areas, only security management had no deficiencies during the review, which covered the security program, assessment and validation of risk, control implementation, awareness and personnel security, monitoring, remediation, or third-party security.

In configuration management, the inspection team identified deficiencies with component inventory, vulnerability management, and the system life cycle. The inspection team found one deficiency regarding system reconstitution in contingency planning controls. While VA's contingency plan addressed control criteria such as identifying essential mission and business functions, provided recovery objectives, and addressed roles and responsibilities, it did not cover the reconstitution of all IT operations after a disaster. Finally, for access controls, the team identified deficiencies in system auditing and physical security.

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. The inspection team reviewed and evaluated the eight configuration management controls drawn from NIST criteria for VA-hosted systems at the Harlingen VA Health Care Center 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. VA should first establish an accurate component inventory to identify all computers on the network.[27] 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 the identified issues, which can include applying patches. This process helps secure computers from attack.

Finding 1: The Harlingen VA Health Care Center Had Deficiencies in Three Configuration Management Controls

To assess configuration management controls, the inspection team interviewed the system owner, information system security officers, system stewards, and personnel from the center's

[27] GAO, *FISCAM*; NIST Special Publication 800-53.

Systems Program Management Office. The team observed system change management processes; reviewed local policies, procedures, and inventory lists; and scanned the center'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 scanned the network to identify vulnerabilities and compared the results to OIT's vulnerability scan results in VA's Information Central Analytics and Metrics Platform.[28] Both the comparisons of the devices and the vulnerability scans showed that OIT did not

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

Additionally, the inspection team found issues with the center's configuration management plan and system life-cycle process. 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 awareness of and control over these systems.[29] A comprehensive view of the components improves a security program by identifying what needs to be managed and secured. The inspection team identified inaccuracies in the component inventory at the Harlingen VA Health Care Center, despite OIT and VA's use of automated inventories of its information systems. VA identified 1,568 devices in the center's inventory. The OIG identified 1,544 devices on the network. However, the component inventory in VA's Enterprise Mission Assurance Support Services (eMASS) identified 942 devices.[30] Because VA's eMASS is used for developing system security and privacy plans, without an accurate inventory of network devices in eMASS, VA has no assurance that these plans implement security controls for all the components within the system.

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

[29] GAO, *FISCAM.*

[30] eMASS is the system VA uses to manage security and privacy risk assessment and authorization activities. It allows for FISMA systems inventory tracking and reporting activities.

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 Harlingen VA Health Care Center. According to the GAO, "Vulnerability assessments involve analyzing a network to identify potential vulnerabilities that would allow unauthorized access to network resources, simulating what might be performed by someone trying to obtain unauthorized access."[31] Vulnerability management is the process by which OIT identifies, classifies, and remediates 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 both routinely and randomly, or when new vulnerabilities are identified and reported.

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 owner. The information system owner or system steward uses the Remediation Effort Entry Form to document mitigation or remediation efforts for each deficiency identified from the scan and provides evidence that the deficiencies have been mitigated within established time frames, which are based on the severity of the vulnerability. VA requires that critical vulnerabilities be remediated within 30 days and high-risk vulnerabilities be remediated in 60 days.

NIST assigns severity levels to vulnerabilities using the Common Vulnerability Scoring System. 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. For example, on a scale of zero to 10, critical vulnerabilities have a score between 9.0 and 10, whereas high-risk vulnerabilities have a score between 7.0 and 8.9.

The inspection team compared OIT's vulnerability scan results from the Harlingen VA Health Care Center with scans the inspection team conducted from January 10 to January 13, 2022. OIT and the team used the same vulnerability-scanning tools. The inspection team identified 16 vulnerabilities—five critical vulnerabilities on less than 1 percent of the computers and 11 high-risk vulnerabilities on 20 percent of the computers—that OIT had identified but not mitigated within OIT's established time frames. The oldest vulnerability was identified on the network in 2013. Further, the computers with critical vulnerabilities also had unsupported operating systems. The OIG also found one critical vulnerability on about 1 percent of computers and six high-risk vulnerabilities on 32 percent of the computers that would have been detectible

[31] GAO, *FISCAM*.

by earlier scans but were not included in prior OIT scan results.[32] Similarly, the prior FISMA audit found that "VA did not have a complete inventory of all vulnerabilities present on locally hosted systems."[33] The inspection team could not determine whether these seven vulnerabilities bypassed detection by VA scanning or were introduced by computers not being vetted for vulnerabilities before being placed on the VA network.[34] 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.

The center did not remediate all flaws affecting devices in its network. The inspection team identified unsupported versions of applications, and missing patches. The flaw remediation process identifies, reports, and corrects system flaws, which includes installing security-related software and firmware updates; security-related updates include patches, service packs, and malicious code signatures. Security patches are usually the most effective way to mitigate software flaw vulnerabilities. According to the 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. Although 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.[35]

System Life-Cycle Management

The inspection team noted that almost 53 percent of the Harlingen center's network switches used operating systems that no longer receive maintenance or vulnerability support from the vendor. Furthermore, the deficient devices did not meet VA baseline configurations. These devices should have been refreshed to vendor-supported systems as part of the system development life cycle, between when the vendor announced support would end and the actual end-of-support date. Baseline configurations are documented and formally reviewed and reflect agreed-on specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future changes to systems that include security and privacy control implementation.[36] The baseline configurations for the network equipment are established by the VA OIT Configuration Control Board. Network devices and IT systems are an

[32] The vulnerabilities had earlier publication dates, which indicated when the scanning software was first able to detect them.

[33] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2021*.

[34] OIT did not detect vulnerabilities the OIG team members saw during their scans, possibly because those systems were not active on the network during OIT scans.

[35] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2021*, Report No. 21-01309-74, April 13, 2022.

[36] NIST Special Publication 800-53.

organization's most critical infrastructure. Upgrading is not just a defensive strategy but a proactive one that protects network stability.

Finding 1 Conclusion

The Harlingen VA Health Care Center did not have accurate component inventories in its security program, a problem that could lead to devices not being managed and secured. Its vulnerability management controls did not ensure a comprehensive patch management process. The system life cycle did not replace applications before systems became unsupported. Without effective configuration management, users do not have adequate assurance that the system and network will perform as intended and to the extent needed to support their missions.

Recommendations 1–3

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

1. Implement a more effective process to maintain consistent inventory information for all network segments.
2. Implement a vulnerability management program that ensures system changes occur within organization timelines.
3. Implement effective system life-cycle processes to ensure network devices meet standards mandated by the VA Office of Information and Technology Configuration Control Board.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 1 through 3. The assistant secretary requested recommendations 1 and 2 be closed due to corrective actions he said were completed. To address recommendation 1, the assistant secretary reported that OIT is implementing physical and logical inventory changes that will result in the Harlingen VA Health Care Center complying with inventory requirements. Regarding recommendation 2, the assistant secretary reported that the VA vulnerability identification, remediation, mitigation, and management rate is 99.85 percent of the vulnerabilities. In response to recommendation 3, the assistant secretary reported that VA has a plan to replace the system to ensure network devices maintain standards mandated by the configuration control board. Appendixes D and E contain the full text of the VA management comments.

OIG Response

For recommendations 1 and 3, the planned corrective actions are responsive to the intent of the recommendations. Although the assistant secretary requested closure of recommendation 1, the target date for corrective actions to be completed enterprise-wide is not until November 30, 2022; therefore, the recommendation will remain open. The OIG will monitor implementation of the planned actions and will close the recommendations when VA provides evidence of addressing the issues identified.

Regarding recommendation 2, OIT provided reports that indicate the agency is remediating a high percentage of vulnerabilities; however, the agency still faces challenges with remediating vulnerabilities within established time frames. The inspection team compared the critical vulnerabilities that were identified in the agency's January 2022 and August 2022 vulnerability scans. The comparison indicated that none of the January vulnerabilities were remediated by August 2022. Further, the number of critical vulnerabilities in August that were not remediated within the established time frames increased to 25 critical vulnerabilities from five critical vulnerabilities on certain computers. Consequently, VA needs to develop reports that will highlight older vulnerabilities not remediated within the established time frames. Because of this increase, with none of the critical vulnerabilities identified in January 2022 remediated within the established timelines, recommendation 2 will remain open. The OIG will monitor implementation of the corrective actions and will close the recommendation when VA provides evidence of addressing the issues identified.

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 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 identifying supporting resources,
- taking steps to prevent and minimize potential damage and interruption,
- establishing a comprehensive contingency plan, and
- periodically testing the contingency plan with appropriate adjustments based on testing.[37]

If contingency planning controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. To determine whether recovery plans will work as intended, 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."[38] Although often referred to as disaster recovery or contingency plans, controls to ensure service continuity should address the entire range of potential disruptions. These may include minor interruptions (e.g., temporary power failures) as well as fires, natural disasters, and terrorism, which would require reestablishing operations at a remote location. To determine if the Harlingen VA Health Care Center met federal guidance and VA requirements, the inspection team evaluated seven contingency planning controls.

The inspection also included a review of locally hosted systems. These systems may include minor applications that, if not part of a general support system, require some level of protection. During the evaluation, the team identified multiple locally hosted systems. Although these systems support the mission, the Harlingen center's personnel indicated that they were not mission essential and said the center could use alternate processes during a disaster.

[37] GAO, *FISCAM*. The FISCAM critical elements for contingency planning are listed in appendix B of this report.
[38] FISMA.

Finding 2: The Harlingen VA Health Care Center Was Deficient in One Contingency Planning Control

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

The inspection team found that the center's policies and procedures addressed control criteria, such as identifying critical operations, implementing environmental controls, and performing preventive maintenance. The team verified that the center had an alternate processing facility and that training and testing were conducted in accordance with policies. Further, the center relied on OIT to continue operations of mission-critical systems during a disaster. However, the inspection team found that the Harlingen VA Health Care Center's contingency plan did not fully address reconstituting all systems to restore IT operations to a fully operational state after a disaster.

System Reconstitution

The inspection team noted that the Harlingen VA Health Care Center's contingency planning documentation indicated that mission-essential major systems were maintained and would be recovered by OIT. However, the contingency documentation did not address local IT operations, including a system used to restrict physical access to sensitive areas and a silent alarm system that alerts police of emergency situations.

The center has multiple local applications that support its mission and is required to provide for the recovery and reconstitution of its information systems to a known state after a failure.[39] The center's representatives indicated that, during a disaster, manual processes could be used in lieu of these systems; however, without adequate plans for system reconstitution, the center may not be able to readily recover all operations should such a disaster actually occur.

Finding 2 Conclusion

The Harlingen VA Health Care Center relies on OIT to continue mission-critical operations in the event of a disaster; however, the center's plans did not address the restoration of local IT operations. Consequently, after a disaster, the center may not be able to readily restore all operations as they existed before. After the OIG brought this to their attention, officials with the Texas Valley Coastal Bend Healthcare System updated the contingency plan to address system reconstitution. Accordingly, the OIG did not make any recommendations for improvement.

[39] NIST Special Publication 800-53; VA Handbook 6500.

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 two security management critical elements: instituting a security management program and assessing and validating risk.[40]

Finding 3: No Weaknesses Were Found in Security Management Controls

The team reviewed local security management policies, standard operating procedures, and applicable VA policies, including documentation from eMASS. The team reviewed how the center handled external media, risk analysis, and plans of action and milestones for known deficiencies. The team also interviewed information system security officers, local administrators, contracting officer's representatives, privacy officers, and system stewards.

The Harlingen VA Health Care Center's security management program has a comprehensive risk assessment process—local policies contained the required information, and the center has appropriate policies and procedures to monitor the activities of third parties. The team did not identify any deficiencies in the center's security management controls. Accordingly, the OIG did not make any recommendations for improvement.

[40] 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. Access controls, including protections for boundaries, 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 Harlingen VA Health Care Center, the inspection team reviewed all six critical access control elements.[41]

Finding 4: The Harlingen VA Health Care Center Had Deficiencies in Three Access Controls

To evaluate the Harlingen VA Health Care Center's access controls, the inspection team interviewed the information system security officer, system stewards, local administrators, and the system owner; reviewed local policies and procedures; conducted walk-throughs of the center; and analyzed audit logs.[42]

The OIG found these issues with access controls:

- Database managers did not adequately maintain log data for local databases.
- Computer rooms and communications closets were not equipped with fire detection devices.
- The center's VA police computer room did not have a visitor access log.

Audit and Monitoring

The OIG determined that improvements are needed for logging administrative actions, retaining logs, and reviewing logs for databases at the Harlingen VA Health Care Center. Audit and monitoring controls involve the collection, review, and analysis of events for indications of inappropriate or unusual activity. These controls should be routinely used to assess the effectiveness of other security controls, recognize an attack, and investigate during or after an attack.[43] The Harlingen VA Health Care Center 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 and 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.

[41] FISCAM critical elements for access controls are listed in appendix B.

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

[43] NIST, *Guide for Security-Focused Configuration Management of Information Systems*, Special Publication 800-128, August 2011; VA Handbook 6500.

Physical Environmental Controls

The Harlingen VA Health Care Center did not employ fire detection devices in its two computer rooms and five communication closets, as required by VA policy.[44] Without these fire detection devices, the center may not be able to readily respond to a fire before the sprinkler systems activate. This could affect the organization's mission, damage organizational assets, and result in financial loss or harm to veterans.

Physical Access

The computer room housing the Harlingen VA Health Care Center's VA police servers did not have a visitor access log. Visitor access logs are required to capture names and organizations of visitors, visitors' signatures, forms of identification, dates of access, entry and departure times, purpose of visits, and the names and organizations of individuals allowing the computer room visit.[45] Without visitor access logs, there is no record of visitors who enter the computer rooms. In the event of intentional or unintentional damage to equipment or the computer room, research into who should be held accountable would be impeded. Center officials implemented visitor access logs in the computer room after the OIG team brought this issue to their attention. Accordingly, the OIG did not make any recommendations for improvement.

Finding 4 Conclusion

The Harlingen VA Health Care Center database audit logs were not properly retained, smoke detectors were not deployed in computer rooms or communication closets, and a computer room did not have a visitor access log. Unless the Harlingen VA Health Care Center takes corrective actions, its ability to respond to incidents may be impeded.

Recommendations 4–5

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

4. Develop and implement a process to retain database logs for a period consistent with VA's record retention policy.

The OIG made the following recommendation to the Harlingen VA Health Care Center director:[46]

[44] NIST Special Publication 800-53; VA Handbook 6500.

[45] NIST Special Publication 800-53; VA Handbook 6500.

[46] The recommendation addressed to the director of the healthcare center is directed to anyone in an acting status or performing the delegable duties of the position.

5. Validate that appropriate physical and environmental security measures are implemented and functioning as intended.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendation 4. The assistant secretary reported that the Database Management Service Line and Network Security Services Team installed a database activity monitoring agent, and VA now retains the required logs for a period consistent with VA's record retention policy.

The Harlingen VA Health Care Center acting director concurred with recommendation 5. The acting director reported that the center has initiated projects to place fire detection systems in the two computer rooms and five communication closets and implement visitor access logs for computer rooms and communication closets.

OIG Response

The assistant secretary reported the corrective actions regarding recommendation 4 were completed and provided sufficient evidence to support his assertion. As a result, the OIG considers recommendation 4 closed.

The Harlingen VA Health Care Center acting director reported the corrective actions regarding recommendation 5 were in progress. The OIG will monitor implementation of the planned actions and will close the recommendation when VA provides evidence of addressing the issues identified.

Overall Conclusion

The OIG recommended that the assistant secretary for information and technology and chief information officer implement (1) a more effective process to maintain consistent inventory information for all network segments, (2) a vulnerability management program that ensures system changes occur within organization timelines, (3) an effective system life-cycle process to ensure network devices meet standards mandated by the VA OIT Configuration Control Board, and (4) a process to retain database logs for a period consistent with VA's record retention policy. The OIG made these recommendations to the assistant secretary because they are related to enterprise-wide IT security issues similar to those identified during previous FISMA audits and IT security reviews. The OIG also recommended that the Harlingen VA Health Care Center director (5) validate that appropriate physical and environmental security measures are implemented and functioning as intended.

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

Appendix A: FISMA Audit for Fiscal Year 2021 Report Recommendations

In the FISMA audit for fiscal year 2021, CliftonLarsonAllen LLP made 26 recommendations. All 26 recommendations were repeated from the prior year. The FISMA audit assesses the agency-wide security management program, and recommendations in the FISMA report are not specific to the Harlingen VA Health Care Center. The 26 recommendations are listed below:

1. Consistently implement an improved continuous monitoring program in accordance with the NIST Risk Management Framework. Specifically, implement an independent security control assessment process to evaluate the effectiveness of security controls prior to granting authorization decisions.
2. Implement improved mechanisms to ensure system stewards and Information System Security Officers follow procedures for establishing, tracking, and updating Plans of Action and Milestones for all known risks and weaknesses including those identified during security control assessments.
3. Implement controls to ensure that system stewards and responsible officials obtain appropriate documentation prior to closing Plans of Action and Milestones.
4. Develop mechanisms to ensure system security plans reflect current operational environments, include an accurate status of the implementation of system security controls, and all applicable security controls are properly evaluated.
5. Implement improved processes for reviewing and updating key security documents such as security plans, risk assessments, and interconnection agreements on an annual basis and ensure the information accurately reflects the current environment.
6. Implement improved processes to ensure compliance with VA password policy and security standards on domain controls, operating systems, databases, applications, and network devices.
7. Implement periodic reviews to minimize access by system users with incompatible roles, permissions in excess of required functional responsibilities, and unauthorized accounts.
8. Enable system audit logs on all critical systems and platforms and conduct centralized reviews of security violations across the enterprise.
9. Implement improved processes for establishing and maintaining accurate data within VA's authoritative system of record 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. 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. 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.[47]
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 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 agency-wide 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 agency-wide awareness of information security events.

[47] Credentialed vulnerability assessments are vulnerability scans performed using a user account and password of an administrator.

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 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** by naming and describing the physical and functional characteristics of a controlled item, as well as by 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.[48] Products should comply with applicable standards and the vendors' good security practices. The organization should have the ability to monitor and test to determine if a system is functioning as intended, as well as to determine if networks are appropriately configured and paths are protected between information systems.
- **Update software on a timely basis** by scanning software and updating it frequently to guard against known vulnerabilities. In addition, security software should be kept current by establishing effective programs for patch management, virus protection, and identification of other emerging threats. Software releases should be controlled to prevent the use of noncurrent software. Examples of these controls are software usage restrictions, user-installed software, malicious code protection, security alerts, and

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

advisories. Examples of controls in this element are vulnerability management, 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 managers to determine which are the most critical and what resources are needed to recover and support them.
- **Backup procedures and environmental controls** help prevent and minimize damage and interruption. 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 accessed.
- **Contingency testing** determines whether plans will function as intended and can reveal important weaknesses that lead 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 managers.

- **Implement security awareness and personnel policies** that provide training for new employees, contractors, and users; periodic refresher training; and distribution of security policies detailing rules and expected behaviors. This element also addresses hiring, transfers, terminations, and performance for employees, contractors, and users. Examples of controls in this area are security awareness training, rules of behavior, position categorization, personnel policies, personnel screening, termination, transfer, access agreements, third-party personnel security, and personnel sanctions.
- **Monitor the program** to ensure that policies and controls effectively reduce risk on an ongoing basis. Effective monitoring involves testing controls to evaluate and determine whether they are appropriately designed and operating effectively. Examples of these controls are security assessments, continuous monitoring, privacy impact assessments, and vulnerability scanning.
- **Remediate information security weaknesses** when they are identified, which involves reassessment of related risks, applying appropriate corrective actions, and doing follow-up monitoring to ensure actions are effective. Agencies develop plans of action 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.[49]

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.
- **Controls over sensitive system resources** are designed to ensure the confidentiality, integrity, and availability of system data, and include things 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

[49] GAO, *FISCAM.*

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 follow:

- Provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.
- Recognize the highly networked nature of the current federal computing environment and provide effective government-wide management and oversight of the related information security risks.
- Provide for development and maintenance of minimum controls required to protect federal information and information systems.
- Provide a mechanism for improved oversight of federal agency information security programs.
- Acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions.
- Recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.[50]

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.

[50] FISMA.

NIST Information Security Guidelines

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

Appendix C: Scope and Methodology

Scope

The OIG team conducted an IT security inspection at the Harlingen VA Health Care Center from January through June 2022. 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, and destruction.

Methodology

To accomplish the objective, the inspection team examined relevant laws and policies and inspected the center and systems for security compliance. Additionally, the team interviewed VA personnel responsible for the center's 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 any policy violations and threats to security.

Internal Controls

The 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 interview questions for the Harlingen VA Health Care Center personnel. The team used the FISCAM controls identified in appendix B of this report to determine the FISMA controls used by VA to protect and secure its information systems. Although similar to the contractor-conducted annual FISMA audits, this review focused on security controls that are implemented at the local level. However, there are some controls that overlap and feature 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 Harlingen VA Health Care Center aligned with the control activities category. Control activities are the actions that

managers establish through policies and procedures to achieve objectives and respond to risks in the internal control system, which includes the entity's information systems. When the team identified control activity deficiencies, team members assessed whether other relevant controls contributed to those deficiencies. The team did not address risk assessment controls because VA's risk management framework is based on NIST security and privacy controls.

Fraud Assessment

The inspection team assessed the risk that fraud and noncompliance with provisions of laws, regulations, contracts, and grant agreements, significant in the context of the inspection objectives, could occur during this inspection. The team exercised due diligence in staying alert to any fraud indicators. The OIG did not identify any instances of fraud or potential fraud during this inspection.

Data Reliability

The inspection team generated computer-processed data by using network-scanning tools. The results of the scans were provided to the OIT Quality Performance and Risk. 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, Assistant Secretary for Information and Technology and Chief Information Officer

Department of Veterans Affairs Memorandum

Date: July 26, 2022

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

Subj: OIG Draft Report: Inspection of Information Technology Security at the Harlingen VA Health Care Center in Texas, Project Number 2022-00973-AE-0047 (VIEWS 07951146)

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 Harlingen VA Health Care Center in Texas* (Project Number 2022-00973-AE-0047).

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

3. For questions regarding OIT's comments to the OIG draft report, please contact the Deputy Chief Information Officer for Quality, Performance and Risk.

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 Harlingen VA Health Care

Center in Texas, Project Number 2022-00973-AE-0047

(VIEWS 07951146)

Recommendation 1: Implement a more effective process to maintain consistent inventory information for all network segments.

Comments: Concur. The Department of Veterans Affairs (VA) Office of Information and Technology (OIT) concurs with the Office of Inspector General (OIG) recommendation. Changes since receipt of audit findings related to accountability (physical) management include:

- Inventory compliance (items updated within the last 365 days) was 96.3% as of June 18, 2022. The expected compliance level is 95%.
- Corporate Data Warehouse is the system of record for system component inventory of physical hardware assets.

Changes since receipt of audit findings related to visibility (logical) management include:

- VA established an enterprise integrated product team to review and analyze scanning deltas and ensure that all network segments are identified to resolve gaps in logical inventory reporting as part of ongoing operational activities (enterprise-wide)
- The Enterprise Mission Assurance Support Service (eMASS) is the system inventory of accredited information systems/Authority to Operate boundaries (enterprise-wide).
- OIT Enterprise Federal Information Security Modernization Act (FISMA) Containerization Asset to Boundary (FCAB) project implementation electronically aligns assets to their new FISMA system boundaries in eMASS. The FCAB project implementation reduces the human factor of manually generating and uploading the asset list to eMASS, allowing easier identification of system owners of device assets, better vulnerability management and future baseline configuration capabilities. The anticipated project rollout completion is November 30, 2022 (enterprise-wide).
- VA updated the Texas Valley accreditation boundary to include infrastructure and storage devices to facilitate scanning and vulnerability remediation based on Internet Protocol range and help prevent duplicate accounting of assets in electronic eMASS inventory (facility-specific).

VA requests closure of recommendation 1. VA presented supporting evidence to OIG as part of an enterprise-level initiative during each inspection.

Recommendation 2: Implement a vulnerability management program that ensures system changes occur within organization timelines.

Comments: Concur. VA OIT concurs with OIG's findings and recommendation related to vulnerability management and flaw remediation. OIG's detected items have since been addressed as part of VA's continuous vulnerability management program, to include Plans of Action and Milestones (POA&M) for associated items that required documented mitigation strategies and/or remediation plans based on the closure of all OIG detected vulnerabilities

Within the timeframe of the overall inspection, VA OIT was able to demonstrate vulnerability identification, remediation, mitigation and management rates at Texas Bend of 99.85% for all critical and high

vulnerabilities. OIT ingested the OIG scan data into the OIT vulnerability management tracking tool and the comparison demonstrated that OIT had the same vulnerabilities with a 0.16% variance; some initial data variance may be detected due to the time difference between VA scans, OIG scans and Provided-by-Client (PBC) scan deliverables.

VA consistently maintains 90% or greater vulnerability management of all critical vulnerabilities across the enterprise. The statistically high percentages provide significant evidence that VA has implemented and is managing an effective vulnerability management and flaw remediation program aligned with federal and industry standards.

VA requests closure of recommendation 2. VA provided supporting evidence in Appendix A, Recommendation 2.

Recommendation 3: Implement effective system life cycle processes to ensure network devices meet standards mandated by the VA Office of Information and Technology Configuration Control Board.

Comments: Concur. VA OIT concurs with the OIG finding regarding vulnerabilities that existed for an extended time. OIG identified a police system at the facility that had an end-of-life operating system and as a result had unaddressed vulnerabilities. The police system is a special purpose system and managed locally at the facility. VA has a plan in place to replace the system. The facility did not have a POA&M in place for the system after the audit was completed. The facility now has a POA&M with mitigation strategies applied and a scheduled completion date.

Expected Completion Date: November 30, 2022. VA provided supporting evidence embedded in the POA&M.

Recommendation 4: Develop and implement a process to retain database logs for a period consistent with VA's record retention policy.

Comments: Concur. The Database Management Service Line and Network Security Services Team installed a database activity monitoring agent, so that VA now retains the required logs for a period consistent with VA's record retention policy.

Completed March 16, 2022. VA requests closure of recommendation 4. VA provided supporting evidence in Appendix A, Recommendation 4.

Recommendation 5: Validate that appropriate physical and environmental security measures are implemented and functioning as intended.

Comments: Concur. VA concurs with the OIG recommendation regarding environmental control tracking and equipment inspection as well as placing a sign-in log at the server room entrance. VA created a POA&M to document condition and track remediation. A project to install smoke detectors in the Harlingen Health Care server room and information technology closets is currently 50% complete with an estimated completion date of October 1, 2022. VA put in place a sign-in log (with proof provided) prior to the auditor's departure via PBC 060. The project to replace the C-Cure access verification system as well as the camera and surveillance systems is 40% complete with an estimated completion date of February 28, 2023.

Expected Completion Date: February 28, 2023. VA provided supporting evidence embedded in the POA&M.

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

Appendix E: VA Management Comments, Director of VA Texas Valley Coastal Bend Healthcare System

Department of Veterans Affairs Memorandum

Date: July 28, 2022

From: VA Texas Valley Coastal Bend HCS Director (00)

Subj: Draft Report/Report Concurrence: Inspection of Information Technology Security at the Harlingen VA Health Care Center, Harlingen, Texas

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

1. This memorandum serves to concur with the recommendations from the Inspection of IT Security at the Harlingen VA Health Care Center as noted in the Draft Report received June 28, 2022.
2. Please see attached action plan for the following recommendations:

Recommendation 5 (a): The Harlingen VA Health Care Center Director validates that appropriate physical and environmental security measures are implemented and functioning as intended.

- Report Comments: Physical Environmental Controls: The center did not have fire detection systems in its two computer rooms and five communication closets.

Recommendation 5 (b): The Harlingen VA Health Care Center Director validates that appropriate physical and environmental security measures are implemented and functioning as intended.

- Report Comments: Physical Access: Police servers did not have a visitor access log (Visitor's access logs are required to capture names and organizations of individuals visiting, visitors' signatures, forms of identification, dates of access, entry and departure times, purpose of visits, and the names and organizations of individuals allowing the computer room visit).

The OIG removed point of contact information prior to publication.

(Original signed by)

Manuela Perales MSN, RN

Chief of QM

Acting Director

Attachment

VHA Inspection of Information Technology Security at the Harlingen VA Health Care Center (VA Texas Valley Coastal Bend Health Care System) Harlingen, Texas	
Recommendation 5 (a):	**The Harlingen VA Health Care Center Director validates that appropriate physical and environmental security measures are implemented and functioning as intended.**
Report Comments	• Physical Environmental Controls: The center did not have fire detection systems in its two computer rooms and five communication closets.
VA Response:	The Harlingen VA Health Care Center (VA Texas Valley Coastal Bend Health Care System) has begun a project for the placement of fire detection systems in its two computer rooms and five communication closets. The Project is in contracting stage and at 50% Completion.
Supporting Documentation:	*[Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG)]*
Status:	Implementation of this recommendation is still in progress with estimated completion date of October 11, 2022.
Recommendation 5 (b):	**The Harlingen VA Health Care Center Director validates that appropriate physical and environmental security measures are implemented and functioning as intended.**
Report Comments	• Physical Access: Police servers did not have a visitor access log (Visitor's access logs are required to capture names and organizations of individuals visiting, visitors' signatures, forms of identification, dates of access, entry and departure times, purpose of visits, and the names and organizations of individuals allowing the computer room visit).
VA Response:	The Harlingen VA Health Care Center (VA Texas Valley Coastal Bend Health Care System) has begun implementation of visitor access log project. This project is in Contracting Stage. Total completion 40%

VHA Inspection of Information Technology Security at the Harlingen VA Health Care Center (VA Texas Valley Coastal Bend Health Care System) Harlingen, Texas	
Supporting Documentation:	*[Additional details regarding activities to address the identified findings have been provided to the Inspector General (IG)]*
Status:	Implementation of this recommendation is still in progress with target completion date of March 10, 2023.

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 Keith Hargrove Shawn Hill Timothy Moorehead Albert Schmidt
Other Contributors	Victoria Coleman Allison Tarmann

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, VA Texas Valley Coastal Bend 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 Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget
U.S. Senate: John Cornyn, Ted Cruz
U.S. House of Representatives: Mayra Flores

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