DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS HEALTH ADMINISTRATION

Inspection of Information Technology Security at the VA Outpatient Clinic in Austin, Texas

INFORMATION TECHNOLOGY INSPECTION

REPORT #20-01485-114

JUNE 22, 2021

MISSION

The mission of the Office of Inspector General is to serve veterans and the public by conducting meaningful independent oversight of the Department of Veterans Affairs.

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

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

www.va.gov/oig/hotline

1-800-488-8244

Executive Summary

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

The fiscal year 2019 FISMA audit made 25 recommendations to VA. Repeat recommendations included addressing deficiencies in configuration management, security management, and access controls.[3] Appendix A details these recommendations. Although VA has taken steps to improve controls, the policies, procedures, and documentation have not been applied consistently across VA's systems. Therefore, in 2020, the OIG started an IT security inspection program. IT inspections help identify whether VA facilities are meeting federal security requirements related to configuration management, physical security, security management, and access controls.[4] They are typically conducted at selected facilities that have not been assessed under the annual audit required by FISMA (each audit focuses on a sample) or at facilities that previously performed poorly. The VA Outpatient Clinic in Austin, Texas, was selected because it was not evaluated during prior OIG-contracted FISMA audits. The OIG conducted this inspection to determine whether the clinic was meeting federal security guidance. The inspection scope and methodology are described in appendix C.

What the Inspection Found

The inspection team focused on four security control areas at the clinic:

1. **Configuration management controls** "identify and manage" security features for all hardware and software components of an information system.[5]

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

[2] Office of Management and Budget (OMB), OMB Circular A-130, "Managing Information as a Strategic Resource," July 28, 2016; Joint Task Force Transformation Initiative, "Security and Privacy Controls for Federal Information Systems and Organizations," *NIST Special Publication 800-53*, rev. 4, National Institute of Standards and Technology, April 2013, includes updates as of January 22, 2015.

[3] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2019,* Report No. 19-06935-96, March 31, 2020.

[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.

2. **Physical security controls** restrict access to computer resources and protect these resources from intentional or unintentional loss or impairment.[6]
3. **Security management controls** "establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of the procedures."[7]
4. **Access controls** provide reasonable assurance that computer resources are restricted to authorized individuals.

The Austin VA Outpatient Clinic Had Deficiencies in Configuration Management Controls

The clinic had security deficiencies in three configuration management controls:

- **Component inventory**: a descriptive record of IT assets in an organization down to the system level.
- **Vulnerability management**: the process by which the Office of Information and Technology (OIT) identifies, classifies, and reduces weaknesses.
- **Patch management**: how OIT acquires, tests, applies, and monitors updates that address security and functionality problems.[8]

The three configuration management controls are interconnected: a complete, accurate, and up-to-date inventory is essential to implement an effective security program.[9] Inaccurate component inventories affect vulnerability and patch management effectiveness. OIT scans for vulnerabilities routinely, randomly, or when new vulnerabilities are identified and reported.[10]

Although the inspection team and OIT used the same vulnerability scanning tools, OIT did not detect all the vulnerabilities identified by the team. Some of the vulnerabilities were present on multiple computers. The team found OIT did not detect 150 of the 246 vulnerabilities, with 23 considered critical and 127 high severity. Additionally, OIT did not provide evidence that there was a patch management plan for the 96 vulnerabilities that both the team and OIT identified.

[6] GAO, FISCAM.

[7] GAO, FISCAM.

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

[9] GAO, FISCAM.

[10] VA Handbook 6500.

Due to the vulnerabilities that OIT did not identify, the inspection team determined that OIT's standard vulnerability identification process and scans were ineffective. The poor component inventories and vulnerability management contributed to inadequate patch management. Despite VA's significant patch management measures, the team identified several devices that were missing patches. Without these controls, VA may be placing critical systems at unnecessary risk of unauthorized access, alteration, or destruction.

The Austin VA Outpatient Clinic Had Deficiencies in Media Protection but No Weaknesses Were Found in Other Physical Security Controls

During its inspection of the clinic, the team identified three hard drives in the biomedical technicians' repair room that potentially held personally identifiable information and personal health information and were not labeled or processed for sanitization. Media protection deficiencies like these increase the risk of unauthorized disclosure of veterans' personally identifiable information and personal health information.[11] The team did not identify deficiencies with the maintenance, physical, or environmental security controls.

No Deficiencies Were Identified for Security Management and Access Controls at the Austin VA Outpatient Clinic

The inspection team did not identify any deficiencies in the security management and access controls for the clinic. Security management controls establish a framework and continuous cycle for assessing risk, developing security procedures, and monitoring the effectiveness of the procedures. Access controls provide reasonable assurance that computer resources are restricted to authorized individuals, while identification and authentication controls ensure that users have the proper access and are uniquely identified. The clinic's existing policies and procedures addressed both security management and access controls.

What the OIG Recommended

The OIG recommended the area manager for the Central Texas Veterans Health Care System maintain an accurate inventory and implement a more effective patch and vulnerability management program. The OIG also recommended distributing the standard operating procedure for media protection to employees who work with media storage and ensuring compliance with

[11] According to VA Handbook 6500, personally identifiable information is information that can be used to distinguish or trace an individual's identity such as their name, Social Security number, and biometric records. Protected health information is individually identifiable health information held by a covered entity or by a business associate acting on its behalf. Within VA, the Veterans Health Administration is the only covered entity. Certain other VA components, such as OIT, are business associates of the Veterans Health Administration.

the procedure's labeling and sanitization provisions. The OIG will monitor VA's progress and follow up on implementation of the recommendations until all proposed actions are completed.

Management Comments

The acting assistant secretary for information and technology and chief information officer provided comments on behalf of the area manager for the Central Texas Veterans Health Care System and concurred with the recommendations. Responsive action plans with target completion dates were provided for each of the three recommendations. Appendix D contains the full text of VA's responses. The OIG will monitor implementation of planned actions and will close the recommendations when VA provides sufficient evidence demonstrating progress in addressing the recommendations and the issues identified.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

Contents

Abbreviations

FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Modernization Act
GAO	Government Accountability Office
IT	information technology
ITOPS	OIT's Information Technology Operations and Services
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information and Technology
OMB	Office of Management and Budget
VHA	Veterans Health Administration

Introduction

The VA Office of Inspector General (OIG) conducted this inspection to determine whether the VA Outpatient Clinic in Austin, Texas, was meeting federal security requirements and complying with related guidance.[12] Security inspections assess the effectiveness of information technology (IT) controls that protect VA systems and data from unauthorized access, use, modification, or destruction. In 2020, the OIG started an IT security inspection program to provide recommendations to VA on enhancing information security oversight at local and regional facilities. This is the IT inspection program's first report.[13]

The Federal Information Security Modernization Act of 2014 (FISMA) was established, in part, to improve oversight of federal agency information security programs.[14] In accordance with the act, VA must develop, document, and implement an agencywide information security and risk management program. FISMA also requires the chief information officers, in accordance with other senior agency officials, to report annually on the effectiveness of the agency's information security program. In addition, FISMA states that inspectors general are required to conduct annual independent evaluations of their respective agencies' information security programs.

The OIG IT inspection program reviews sites not evaluated under the annual FISMA audits (as only a sample of facilities are examined) or facilities that did not perform well in prior FISMA audits. The inspection team selected the Austin clinic because it was not evaluated during prior OIG-contracted FISMA audits. The clinic was the first of seven sites to be inspected in 2020. However, the team postponed the remaining inspections due to COVID-19 pandemic restrictions on the team's ability to conduct in-person evaluations of VA facilities. As the first site, the Austin clinic provided the OIG with the opportunity to perform a limited assessment of controls and to gather information that will be used to tailor future inspection processes and procedures.

The OIG's IT inspections are not intended to duplicate the OIG's FISMA audits. However, there is some redundancy in the controls that are assessed for both due to overlapping roles and responsibilities among VA's local, regional, and national facilities and offices. The IT inspections are focused on four security control areas outlined in guidance developed by the

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

[13] 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.

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

Government Accountability Office (GAO) that apply to local facilities and were selected based on their level of risk:[15]

1. **Configuration management controls** "identify and manage" security features for all hardware and software components of an information system.
2. **Physical security controls** restrict access to computer resources and protect these resources from intentional or unintentional loss or impairment.
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."
4. **Access controls** provide reasonable assurance that computer resources are restricted to authorized individuals.

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

Security Controls

Both the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) provide criteria to evaluate security controls. These criteria provide specific requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system.[16] Figure 1 details the criteria assessed in OIG IT inspections.

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

1. Configuration Management Controls	"Identify and manage" security features for all hardware and software components of an information system. *Controls evaluated: component inventory, vulnerability management, and patch management*
2. Physical Security Controls	Restrict access to computer resources and protect these resources from intentional or unintentional loss or impairment. *Controls evaluated: media marking, media sanitization, maintenance, physical, and environmental*
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." *Controls evaluated: personnel security*
4. Access Controls	Provide reasonable assurance that computer resources are restricted to authorized individuals. *Controls evaluated: access, identification, authentication, audit, and accountability*

Figure 1. *Security controls evaluated in this report.*
Source: VA OIG analysis.

According to VA Handbook 6500, the responsibility for developing and maintaining information security policies, procedures, and control techniques lies with the assistant secretary for IT, who is also VA's chief information officer. VA guidance provides the risk-based process for selecting system security controls, including the operational requirements.[17] VA established guidance outlining both NIST and VA-specific requirements to help information system owners select the appropriate controls to secure their systems.

Office of Information and Technology Structure and Responsibilities

The assistant secretary for information and technology and chief information officer leads the Office of Information and Technology (OIT). OIT delivers available, adaptable, secure, and cost-

[17] VA Handbook 6500, *Risk Management Framework for VA Information Systems–Tier 3: VA Information Security Program*, March 2015.

effective technology services to VA and acts as a steward for VA's IT assets and resources. The Cybersecurity Operations Center is part of OIT's Office of Information Security. It is responsible for protecting VA information and information systems by identifying and reporting emerging and imminent threats and vulnerabilities. OIT's Information Technology Operations and Services (ITOPS) provides standardized customer service, technology implementation, and technical support. There are three ITOPS offices involved in local information security practices:

- **Solution Delivery**. Personnel manage configuration requirements at the national level to facilitate the implementation of configuration management policies and controls. Solution Delivery also establishes configuration baselines for products. Finally, Solution Delivery employs automated mechanisms to centrally manage, automate, and verify configuration settings for information system components such as laptops, workstations, databases, and servers.
- **Patch and Vulnerability Team**. This office distributes information regarding threats and vulnerabilities as well as available solutions, which may include applying patches. In accordance with the Patch and Vulnerability Team's procedures, OIT uses automated patch management tools across its enterprise to speed up the distribution of patches to systems.[18] Information systems owners and the deputy chief information officer for service delivery and engineering maintain and organize the team.
- **End User Operations**. Staff execute local systems implementation and engage with VA customers across the nation to meet IT support needs. End User Operations provides on-site and remote support to IT customers. At the time of the OIG inspection, the Central Texas Veterans Health Care System had 44 personnel supporting the healthcare system, which included three specialists at the Austin clinic. Local site personnel also correct systems issues that cannot be centrally automated.

Figure 2 shows the organizational structure of the entities relevant to this inspection.

[18] VA Handbook 6500.

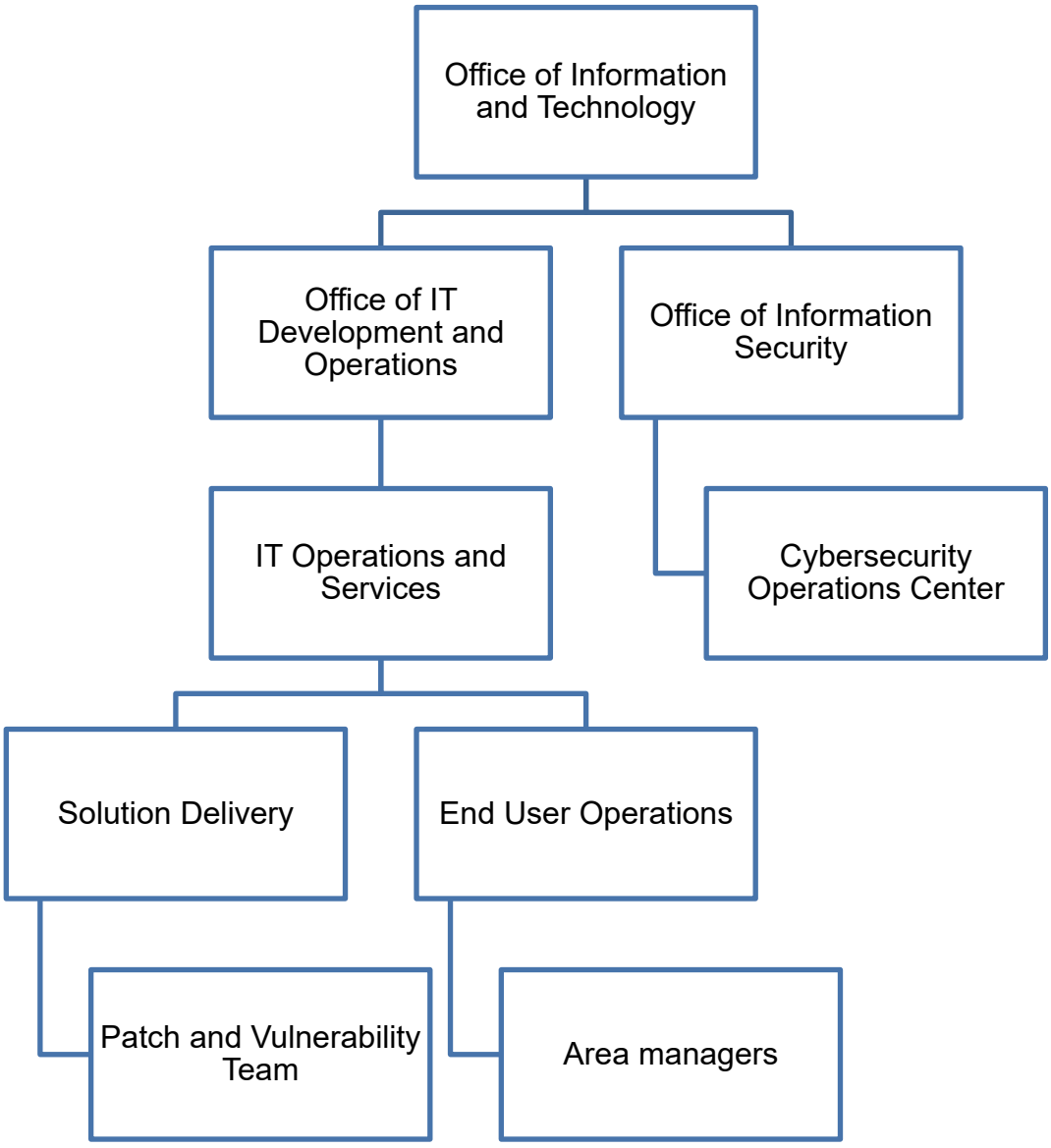

Figure 2. *Organizational structure of entities relevant to this inspection.*

Source: VA OIG analysis.

Prior OIG FISMA Audit

The OIG issues annual reports on VA's information security program based on audits conducted by the independent public accounting firm CliftonLarsonAllen LLP. The fiscal year 2019 FISMA audit included an evaluation of 49 major applications and general support systems hosted at 24 VA facilities, including the testing of selected management, technical, and

operational controls outlined by NIST.[19] CliftonLarsonAllen LLP made 25 recommendations, which are listed in appendix A. Based on the 24 repeat recommendations from the prior annual audit, the OIG concluded that VA continues to face significant challenges in complying with FISMA.[20] Although VA has taken steps to improve controls, the policies, procedures, and documentation have not been applied consistently across VA's systems.

Related Government Accountability Office Review

A November 2019 GAO review also found that VA was one of the federal agencies that continued to have a deficient information security program.[21] According to the GAO, VA faced several security challenges as it secured and modernized its information systems:

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

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

Austin VA Outpatient Clinic

Since opening in 2013, the Austin VA Outpatient Clinic (figure 3) has served the healthcare needs of veterans in Austin and the surrounding area. As VA's largest freestanding outpatient clinic, it conducts almost 300,000 outpatient visits annually.[23] Without an effective information security program, VA could be putting the personally identifiable information and personal health information of patients, dependents, beneficiaries, VA employees, contractors, or

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

[20] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2019,* Report No. 19-06935-96. March 31, 2020. Appendix B provides background on federal information security.

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

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

[23] Veterans Health Administration, Central Texas Veterans Health Care System (website), Austin VA Clinic, accessed August 6, 2020, https://www.centraltexas.va.gov/locations/Austin.asp; and OIG analysis.

volunteers at risk of loss, unauthorized disclosure, improper modification, and inadvertent or deliberate misuse or destruction.[24]

Figure 3. *The Austin VA Outpatient Clinic.*

Source: VA website, accessed March 17, 2020, https://www.centraltexas.va.gov/locations/Austin.asp.

[24] According to VA Handbook 6500, personally identifiable information is information that can be used to distinguish or trace an individual's identity such as their name, Social Security number, and biometric records. Protected health information is individually identifiable health information held by a covered entity or by a business associate acting on its behalf. Within VA, the Veterans Health Administration is the only covered entity. Certain other VA components, such as OIT, are business associates of the Veterans Health Administration.

Results and Recommendations

The inspection team reviewed configuration management, physical security, security management, and access controls at the Austin clinic. Some of these controls depend on locally hosted systems. If there are no locally hosted systems, the controls are inherited from OIT's general support systems. General support systems are evaluated during the OIG's annual contracted FISMA audits. Within configuration management, the team identified deficiencies in component inventory, vulnerability management, and patch management. Because the team did not identify any locally hosted systems, baseline configuration and change controls were not applicable.

During the evaluation of the physical security controls, the inspection team identified deficiencies with media marking (labeling) and sanitization controls. The team did not identify any deficiencies in maintenance, physical, or environmental security controls.

The inspection team's review of security management controls focused on personnel security. The lack of locally hosted systems at the Austin clinic meant evaluations were not performed for security assessments, security planning, risk assessments, and authorization controls. The team did not identify any deficiencies in personnel security controls at the Austin clinic; therefore, the OIG did not make any recommendations in these areas.

Finally, the inspection team reviewed access controls that include user identification, authentication, audit, and accountability elements. As the team did not identify any weaknesses in the access controls at the Austin clinic, the OIG made no related recommendations.

Configuration Management Controls

According to the GAO's *Federal Information System Controls Audit Manual*, configuration management identifies and controls IT hardware and software security features. The inspection team evaluated three configuration management controls for VA-hosted systems (drawn from NIST and VA criteria) at the Austin VA Outpatient Clinic to determine if they met federal guidance and VA requirements.[25]

- **Component inventory**: a descriptive record of IT assets in an organization down to the system level
- **Vulnerability management**: the process by which OIT identifies, classifies, and reduces weaknesses

[25] Joint Task Force Transformation Initiative, "Security and Privacy Controls for Federal Information Systems and Organizations," *NIST Special Publication 800-53*, rev. 4, National Institute of Standards and Technology, April 2013, includes updates as of January 22, 2015; VA Handbook 6500.

- **Patch management**: how OIT acquires, tests, applies, and monitors updates that address security and functionality problems[26]

To achieve effective configuration management, VA must first establish an accurate component inventory to identify all computers on the network.[27] Component inventories affect the success of 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 for remediations which address identified issues and may include applying patches. This process helps secure computers from attack.

The OIG's IT inspections also include a review of locally hosted systems, if applicable.[28] These systems may include minor applications that, if not part of a general support system, require some level of protection.[29] As the inspection team did not identify any locally hosted systems at the Austin clinic, these controls were not evaluated. The clinic's controls were inherited from VA's general support system. General support system controls are assessed in the annual FISMA audits.

Finding 1: The Austin VA Outpatient Clinic Had an Inaccurate Component Inventory and Deficiencies in Vulnerability and Patch Management

To assess configuration management controls, the inspection team interviewed the area manager, local administrators, and biomedical technicians; reviewed local policies, procedures, and vulnerability lists; and scanned the Austin clinic's network to identify devices and vulnerabilities.[30] A comparison of the OIT and team scans showed that VA

- did not accurately identify all components in the Austin VA Outpatient Clinic's network,
- did not identify all critical or high-risk vulnerabilities in the network, and
- did not apply several required system patches.

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

[27] GAO, FISCAM.

[28] Joint Task Force Transformation Initiative, "Security and Privacy Controls for Federal Information Systems and Organizations." Where there are locally based systems, these additional controls are examined. Baseline configuration examines the documented, formally reviewed, and agreed-upon sets of specifications for information systems. Change control involves a systematic approach to managing modifications to an information system. Finally, configuration management plans document and manage changes to an information system.

[29] Joint Task Force Transformation Initiative, "Security and Privacy Controls for Federal Information Systems and Organizations." This document details the NIST controls (SP 800-53).

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

Although the inspection team did not identify any locally hosted systems at the Austin clinic for evaluation, it found that VA's policies and procedures for its general support systems addressed control criteria such as establishing a configuration management plan, controlling baseline configurations, and implementing a change control process. However, by not implementing more effective security 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. A complete, accurate, and up-to-date inventory is essential to implement an effective information security program by providing greater visibility into and control over these systems.[31] 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 Austin VA Outpatient Clinic, despite OIT and VA's use of automated systems to maintain a readily available baseline of its information systems. The area manager for the Central Texas Veterans Health Care System identified 944 components in the Austin clinic's inventory. However, the team identified 1,985 components.

Vulnerability Management

Prior FISMA audits also repeatedly found deficiencies in VA's vulnerability assessments. Consistent with those findings, the inspection team identified weaknesses in vulnerability management at the Austin VA Outpatient Clinic. According to the GAO, "vulnerability assessments involve analyzing a network to identify potential vulnerabilities that would allow unauthorized access to network resources and then simulating what someone might do to obtain unauthorized access."[32] Unidentified threats cannot be mitigated; they represent weaknesses that could be exploited to gain access to VA data. Management personnel, therefore, should periodically perform assessments to protect information, address vulnerabilities, and make decisions about accepting or mitigating risks.[33]

[31] GAO, FISCAM.

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

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 provides a way to capture the principal characteristics of a vulnerability and produces a numerical score reflecting its severity. Numerical scores are classified as low, medium, high, or critical to help organizations properly assess and prioritize their vulnerability management processes. For example, on a scale of 0 to 10, critical vulnerabilities have a score between 9.0 and 10, while high vulnerabilities have a score between 7.0 and 8.9. OIT establishes time frames for remediating vulnerabilities based on their severity.

OIT provided network vulnerability scan results from the Austin Outpatient Clinic to the inspection team on February 25, 2020. The team conducted scans of the same network from February 24 through 28, 2020. The team and OIT used the same vulnerability scanning tools. The team identified 246 vulnerabilities—101 critical vulnerabilities on 24 computers and 145 high vulnerabilities on 45 computers—which were not mitigated within the time frames established by OIT. The team identified vulnerabilities such as operating systems that are no longer supported and applications with missing patches. Unsupported operating systems may become less secure over time as vendors no longer release updates and patches to remedy emerging vulnerabilities. Missing patches can expose systems to security and functionality problems. Some vulnerabilities were present on multiple computers. As seen in figure 4, the team found OIT did not detect 150 of the 246 vulnerabilities, with 23 scored as critical and 127 as high severity.

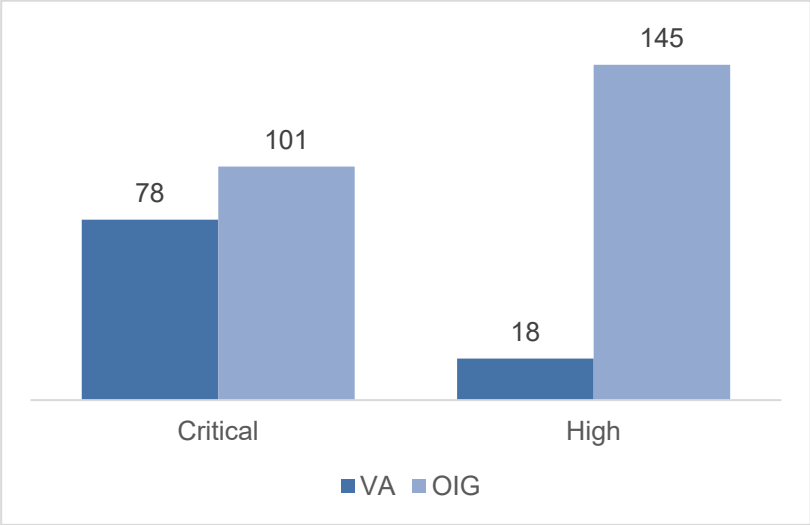

Figure 4. *Vulnerabilities identified by VA and the inspection team.*
Source: VA OIG analysis.

[34] "Vulnerability Metrics," NIST, accessed August 21, 2020, https://nvd.nist.gov/vuln-metrics/cvss; "Common Vulnerability Scoring System version 3.14 Specification Document Revision 1," Forum of Incident Response and Security Teams (FIRST), accessed March 13, 2020, https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf.

The inspection team did not receive evidence that there was a patch management plan for several vulnerabilities that both the team and OIT identified.

The Cybersecurity Operations Center identifies and reports threats and vulnerabilities for VA. In addition, OIT conducts scans for vulnerabilities routinely, randomly, or when new vulnerabilities are identified and reported.[35] However, due to the vulnerabilities that OIT did not identify, the inspection team determined that the scans were inadequate.

Patch Management

The Austin VA Outpatient Clinic provided a patch management plan for medical equipment with software at the facility; however, there was not a plan for nonmedical devices such as servers and workstations. According to the GAO, a patch is a piece of software code inserted into a program to temporarily fix a defect. NIST further explains that patches correct security and functionality problems in software and firmware.[36] Patches are usually the most effective way to mitigate software flaw vulnerabilities and are often the only fully effective solution. Although patch management is a critical process used to help alleviate many of the challenges involved with securing systems from cyberattack, previous FISMA audits have repeatedly found deficiencies in this area.[37]

Patch management includes acquiring, testing, applying, and monitoring patches to a computer system. In accordance with the Patch and Vulnerability Team's procedures, OIT uses automated patch management tools across its enterprise to speed up the distribution of patches to systems. The Infrastructure Operations Security Management Office established a permanent enterprise patch and vulnerability program in June 2017. The program identifies, remediates, and mitigates vulnerabilities. OIT's Patch and Vulnerability Team distributes information regarding threats and vulnerabilities as well as available solutions, which may include applying patches. If patches cannot be applied using automated tools, a notification is sent to End User Operations technicians to apply patches and update systems. Despite VA's significant patch management measures, the inspection team identified several devices that were missing patches. 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.

Finding 1 Conclusion

The Austin VA Outpatient Clinic did not have accurate inventories, which led to critical and high-severity vulnerabilities in its systems not being detected or remediated. Inaccurate

[35] VA Handbook 6500. Appendix B provides additional information about federal criteria and standards discussed in this report.

[36] 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.

[37] GAO, FISCAM.

inventories and ineffective vulnerability assessments prevented an effective patch management program, which is required to mitigate security flaws in VA systems within time frames determined by OIT.

Recommendations 1–2

The OIG made the following recommendations to the area manager for the Central Texas Veterans Health Care System:

1. Implement more effective automated inventory management tools.
2. Implement a more effective patch and vulnerability management program that can accurately identify vulnerabilities and enforce patch application.

Management Comments

The acting assistant secretary for information and technology and chief information officer concurred with recommendations 1 and 2 and provided comments on behalf of the area manager for the Central Texas Veterans Health Care System. In response to recommendation 1, the acting assistant secretary stated VA is in the process of replacing its inventory systems with the Defense Medical Logistics Standard Support system, a product developed by the Department of Defense. The system's asset inventory will include all procured items; it is not limited to IT-related devices. Additionally, biomedical engineering and VHA logistics staff are audited by accreditation agencies and through internal VA processes to ensure all inventory is accurate. VA is also utilizing an automated tool that provides asset management for network-connected specialized devices. Ultimately, this agentless solution will provide full visibility, vulnerability discovery, and remediation management for isolated specialized devices, including medical devices, special-purpose systems, and research scientific computing devices. The Networked Medical Device Database and the Special Purpose System Database provide data inputs to the tool, allowing for additional asset management information and categorization.

VA has also initiated testing and deployment of a specialized device asset management solution under the Internet of Medical Things project which already provides direct security support for COVID-19 vaccine administration. Finally, VA has implemented a Network Access Control System that requires any device to be authorized before network communication is allowed. This system will work with the Internet of Medical Things solution and other inventory systems to ensure nothing is added to the inventory without approval and is accounted for in the system or record.

In response to recommendation 2, the acting assistant secretary stated VA maintains a continuous approach to identification and patching (remediation) of security deficiencies. The Improvement of Patch and Vulnerability Management Program identified gaps in procedures and oversight practices. As a result, workgroups at the strategic, tactical, and operational levels were

established to define governance, perform gap analysis, and establish operational process solutions. As a result, additional identification, automation, and compliance-driven patch efforts will be applied to network infrastructure, database platforms, and web application servers. System-level processes and procedures are also being identified to address deficiencies in the defined vulnerability management ecosystem.

The agency web application security testing program is primarily performed on a system or application basis. However, the Cyber Security Operations Center has expanded this program to include quarterly testing for unsecure web components, common vulnerabilities associated with web services, and unsecure default configurations throughout the enterprise. OIT continues to mature its patch and vulnerability management program, addressing standardization across the enterprise and improving processes for provisioning, testing, and deployment of patches, fixes, and hardening of systems throughout the VA enterprise network.

OIG Response

The corrective actions planned by the acting assistant secretary for information and technology and chief information officer are responsive to the intent of the recommendations. The OIG will monitor implementation of the planned actions and will close the recommendations when VA provides sufficient evidence demonstrating progress in addressing the issues identified. The full text of the responses from the acting assistant secretary is included in appendix D.

Physical Security Controls

Physical security controls protect resources from damage or unauthorized in-person access. As described more fully below, for the purpose of this report physical security controls consist of media protection, maintenance of systems and software, protective measures to limit in-person contact with computer resources, and environmental controls. The term "media" refers to data stored in digital forms, such as on disk drives and external hard drives, and in nondigital forms, such as paper documents. Specifically, the inspection team evaluated the following physical security controls at the Austin VA Outpatient Clinic to determine if they met federal and VA policy requirements:

- **Media marking**: labeling items to indicate distribution limitations, handling conditions, and security attributes (and as part of the sanitization process)
- **Media sanitization**: removing data from items
- **Maintenance controls**: preventing equipment failure or malfunction and restoring operating capability within approved time frames that follow manufacturer specifications or organizational requirements
- **Physical controls**: restricting access to computer resources and protecting them from loss or impairment
- **Environmental controls**: preventing damage or interruptions in service (including activities such as maintaining fire suppression systems, smoke or water detectors, redundant cooling systems, and backup power supplies)[38]

Finding 2: The Austin VA Outpatient Clinic Had Deficiencies in Media Protection but No Weaknesses Were Found in Other Physical Security Controls

During its inspection, the team interviewed the area manager, local administrators, biomedical technicians, and contracting officer's representatives. The team conducted multiple walk-throughs of the facility to identify deficiencies. The team also retrieved and reviewed local policies, procedures, and physical access logs.

Media Marking and Sanitization

The inspection team identified three hard drives in the biomedical technicians' office that were from a physician's defunct mammogram-reading station that potentially held personally identifiable information and personal health information and were not labeled or processed for

[38] FISMA; NIST guidance; VA's IT security policies.

sanitization. A biomedical technician had originally planned to reuse the hard drives. However, after the team discovered them, he decided to turn in the hard drives for destruction.

To protect information, staff should properly label media to identify data sensitivity and distribution limitations. Before disposing of or releasing storage media, VA is required to remove information using techniques and procedures specific to the information's sensitivity.[39] According to NIST, improperly sanitized media could result in unauthorized disclosure of information.[40] For VA this includes veterans' personally identifiable information and personal health information. The regional Central Texas Veterans Health Care System has a media protection standard operating procedure that states that facility biomedical engineering sanitization support specialists should label removed hard drives as part of the media sanitization process. According to the procedure, the chief biomedical engineer is responsible for ensuring that biomedical staff are properly trained in media sanitization procedures and comply with standard operating procedures for protecting media.

Maintenance, Physical, and Environmental Security

The inspection team did not identify deficiencies with the maintenance, physical, or environmental security controls at the Austin VA Outpatient Clinic. The team retrieved and reviewed local standard operating procedures, access logs, and other applicable VA and Veterans Health Administration policies. The team also interviewed the area manager, regional contracting officer's representatives, and local administrators, biomedical technicians, and account management personnel. Additionally, the team conducted walk-throughs of IT rooms and biomedical spaces in the facility.

The inspection team found that

- local policies contained the required information;
- physical controls were in place to prevent unauthorized access to VA information equipment and infrastructure;
- environmental controls were in place to ensure IT equipment maintained proper temperature and humidity and to provide for emergencies such as fire detection and suppression; and
- heating, ventilation, and air-conditioning services for the facility were provided by a contractor whose system does not use the VA IT infrastructure for communication.

[39] VA Handbook 6500.

[40] NIST, "Guidelines for Media Sanitization," *NIST Special Publication 800-88*, Department of Commerce, December 2014.

Finding 2 Conclusion

The inspection team identified security deficiencies at the Austin VA Outpatient Clinic regarding media that were not labeled or processed for sanitization, increasing the risk of unauthorized disclosure of veterans' personally identifiable information and personal health information. The team did not identify deficiencies with maintenance, physical, or environmental security controls.

Recommendation 3

The OIG made the following recommendation to the area manager for the Central Texas Veterans Health Care System:

3. Ensure compliance with the media protection standard operating procedure for all employees who work with media storage and ensure compliance with marking and sanitization provisions.

Management Comments

The acting assistant secretary for information and technology and chief information officer concurred with recommendation 3, provided comments on behalf of the area manager for the Central Texas Veterans Health Care System, and provided remediation details. According to the management comments, the area manager for the Central Texas Veterans Health Care System and the chief biomedical engineer distributed the media protection standard operating procedure to all employees working with media storage and ensure compliance with its labeling and sanitization provisions. This action was completed with the updated standard operating procedure on April 12, 2021.

OIG Response

The corrective actions taken and planned by the local facility are responsive to the intent of the recommendation. The OIG will close the recommendation when VA provides sufficient evidence demonstrating progress in addressing the issues identified. The full text of the responses from the acting assistant secretary is included in appendix D.

Security Management Controls

According to the *Federal Information System Controls Audit Manual*, security management controls establish a framework and continuous cycle for assessing risk, developing security procedures, and monitoring the effectiveness of the procedures. As the inspection team did not identify any locally hosted systems at the Austin clinic, security assessments, security planning, risk assessments, and authorization controls were not evaluated.[41] The clinic's controls are inherited from the VA general support system and are assessed in the annual FISMA audit. The team examined personnel security controls at the Austin VA Outpatient Clinic to determine if they met federal and VA policy requirements. These personnel security processes involve screening individuals before providing access to resources.[42]

During its inspection, the team retrieved and reviewed standard operating procedures for local personnel security, a position risk matrix, privacy inspection logs, and applicable VA and Veterans Health Administration policies. The team retrieved similar documentation from the Enterprise Mission Assurance Support Service, which is VA's cybersecurity management service for workflow automation and continuous monitoring. The team interviewed the area manager, local administrators, contracting officer's representatives, human resources staff, privacy officers, biomedical technicians, and local account management personnel.

Part of the personnel security process is assigning risk to positions and conducting screening according to data the user will access. Personnel security controls also provide criteria for removing secure access for transferred or terminated employees and contracted personnel.

Finding 3: Personnel Security Management Controls Were Sufficient

The Austin clinic's local policies contained the required information, the clinic had a position risk matrix that guided staff conducting position risk designations, and a process was in place for onboarding and terminations. As the inspection team did not identify any reportable deficiencies in personnel security at the Austin VA Outpatient Clinic, no recommendations are made in this area.

[41] For locally hosted systems, the OIG considers four controls: (1) Security assessments involve testing or evaluating controls to determine if they are implemented correctly, operating as intended, and producing the desired outcome. (2) Security plans are formal documents that provide an overview of the security requirements for the systems and describe the controls to meet those requirements. (3) Risk assessments identify and analyze the probability that a particular security threat will exploit a system vulnerability. (4) Authorizations are the official management decisions to allow operation and accept risk for an information system. See Joint Task Force Transformation Initiative, "Security and Privacy Controls for Federal Information Systems and Organizations."

[42] GAO, FISCAM.

Access Controls

Access controls provide reasonable assurance that computer resources are restricted to authorized individuals, while identification and authentication controls ensure that users have the proper access and are uniquely identified.

- **Access controls** limit or detect access to computer resources, protecting them against unauthorized modification, loss, or disclosure by determining the actions that legitimate users are allowed to take in a system.[43] Access controls include account management, separation of duties, and "least privilege" controls.[44]
- **Identification controls** distinguish one user from another.
- **Authentication controls** establish the validity of a user's claimed identity.

Audit and monitoring controls define what events may violate a security policy.[45] The controls are applied to the information systems that identify the event, establish a record of it, and generate reports.[46]

- **Audit controls** define which events a system should record and how the records are retained.
- **Accountability controls** trace activities on a system to individuals who may then be held responsible for their actions.

The inspection team conducted interviews with the area manager, local administrators, contracting officer's representatives, human resources staff, privacy officers, biomedical technicians, and local account management personnel to assess these controls. During its walk-throughs, the team watched biomedical personnel interact with medical devices to determine how access was provided.

Finding 4: No Weaknesses Were Found in Access Controls

Policies and procedures addressed control criteria such as appropriate account management, access enforcement, separation of duties, least privilege, and remote access. As the inspection

[43] NIST, "Assessment of Access Control Systems," *Interagency Report 7316*, Department of Commerce, September 2006.

[44] According to FISCAM and VA Handbook 6500, account management includes the creation, change, and deletion of accounts. Separation of duties means no one individual controls all critical stages of a work process, subsequently reducing the risk of malicious activity in a system. Least privilege allows authorized users only the access necessary to accomplish assigned duties.

[45] GAO, FISCAM.

[46] GAO, FISCAM. An auditable event is a system activity identified by the entity's audit monitoring system that may be indicative of a violation of security policy. The activity may range from simple browsing to attempts to plant a Trojan horse or gain unauthorized access privilege.

team did not identify any deficiencies in the Austin clinic's access, identification, and authentication controls, the OIG is not making any recommendations.

The inspection team also did not find weaknesses in the audit and accountability controls at the Austin VA Outpatient Clinic after reviewing policies and procedures and interviewing appropriate personnel. The Austin clinic's existing policies and procedures addressed auditable events and responsible parties.

Conclusion

The inspection team expected the Austin clinic to be the first of seven sites inspected in 2020. However, due to the COVID-19 pandemic, the team was unable to conduct additional in-person inspections of VA facilities. The clinic provided the team with the opportunity to perform a limited assessment of controls and gather information to shape future inspection processes and procedures.

The inspection team identified deficiencies in configuration management and physical security related to component inventory, vulnerability and patch management, and media marking and sanitization. The OIG made two recommendations to the area manager for the Central Texas Veterans Health Care System related to configuration management: implement more effective automated inventory management tools and implement a more effective patch and vulnerability management program that is able to accurately identify vulnerabilities and enforce patch applications. The OIG also recommended ensuring employee compliance with the media protection standard operating procedure. The team did not identify any deficiencies in the remaining areas evaluated.

Although the information and recommendations in this report are based on findings specific to the Austin clinic, such as improving inventory accuracy and patch and vulnerability management, it is hoped that other facilities within the healthcare system and across VA can benefit from reviewing the information and considering the recommendations.

Appendix A: FISMA Audit for Fiscal Year 2019 Report Recommendations

In the FISMA audit for fiscal year 2019, CliftonLarsonAllen LLP made 25 recommendations to VA's assistant secretary for information and technology. Of these, 24 were repeat recommendations from the prior year. Modified repeat recommendations are marked with an asterisk.

1. Consistently implement an improved continuous monitoring program in accordance with the NIST Risk Management Framework. Specifically, implement an independent security control assessment process to evaluate the effectiveness of security controls prior to granting authorization decisions.*
2. Implement improved mechanisms to ensure system stewards and information system security officers follow procedures for establishing, tracking, and updating Plans of Action and Milestones for all known risks and weaknesses including those identified during security control assessments.*
3. Implement controls to ensure that system stewards and responsible officials obtain appropriate documentation prior to closing Plans of Action and Milestones.*
4. Develop mechanisms to ensure system security plans reflect current operational environments, include an accurate status of the implementation of system security controls, and all applicable security controls are properly evaluated.
5. Implement improved processes for reviewing and updating key security documents such as security plans and interconnection agreements on an annual basis and ensure the information accurately reflects the current environment.*
6. Implement improved processes to ensure compliance with VA password policy and security standards on domain controls, operating systems, databases, applications, and network devices.
7. Implement periodic reviews to minimize access by system users with incompatible roles, permissions in excess of required functional responsibilities, and unauthorized accounts.
8. Enable system audit logs on all critical systems and platforms and conduct centralized reviews of security violations across the enterprise.
9. Fully implement two-factor authentication to the extent feasible for all user accounts throughout the agency.
10. Implement more effective automated mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and web application servers.

11. 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.
12. Maintain a complete and accurate security baseline configuration for all platforms and ensure all baselines are appropriately implemented for compliance with established VA security standards.
13. Implement improved network access controls that restrict medical devices from systems hosted on the general network.*
14. 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.
15. Implement improved processes to ensure that all devices and platforms are evaluated using credentialed vulnerability assessments.
16. Implement improved procedures to enforce standardized system development and change control processes that integrates information security throughout the life cycle of each system.
17. Review system boundaries, recovery priorities, system components, and system interdependencies and implement appropriate mechanisms to ensure that established system recovery objectives are met.*
18. Implement more effective agencywide incident response procedures to ensure timely notification, reporting, updating, and resolution of computer security incidents in accordance with VA standards.
19. Ensure that VA's Cybersecurity Operations Center has full access to all security incident data to facilitate an agencywide awareness of information security events.
20. Implement improved safeguards to identify and prevent unauthorized vulnerability scans on VA networks.
21. Implement improved measures to ensure that security control deficiencies are tracked individually instead of consolidating security deficiencies under one control.*
22. 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.
23. Develop a comprehensive inventory process to identify connected hardware, software, and firmware used to support VA programs and operations.

24. Implement improved procedures for monitoring contractor-managed systems and services and ensure information security controls adequately protect VA sensitive systems and data.*
25. Ensure appropriate levels of background investigations be completed for all personnel in a timely manner, implement processes to monitor and ensure timely reinvestigations on all applicable employees and contractors, and monitor the status of the requested investigations.

Appendix B: Background

Federal Information System Controls Audit Manual

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

Federal Information Security Modernization Act of 2014

The stated goals of FISMA 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.[47]

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 Transformation Initiative Working Group created the NIST information security guidelines.

[47] FISMA.

Appendix C: Scope and Methodology

Scope

The inspection team conducted its work from February 2020 through March 2021. The team inspected the Austin VA Outpatient Clinic during the week of February 24, 2020. The team visited the site prior to the restrictions related to the Centers for Disease Control and Prevention's issuance of guidance on COVID-19 safety. The team evaluated configuration management, physical security, security management, and access controls of operational VA IT assets and resources in accordance with VA's IT security policy, FISMA, and NIST security guidelines. The team also 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 conducted interviews of VA personnel responsible for the Central Texas Veterans Health Care System IT security and operations, privacy compliance, and human resources management. The team conducted vulnerability and configuration testing to determine local systems' security compliance. Finally, the team analyzed the results of testing, interviews, and the inspection to identify policy violations and threats to security.

Internal Controls

The inspection team determined that internal controls were significant to the inspection objectives. The overall scope of IT security inspections is the evaluation of general security and application controls that support VA's programs and operations. According to the risk management framework for VA information systems, the information security program is the foundation for VA's information security and privacy program and practices. The framework is documented in VA Handbook 6500. The team obtained an understanding of relevant internal controls, then assessed and evaluated the controls applicable to the inspected site.

In planning the inspection, the team identified the GAO's *Standards for Internal Control in the Federal Government* components significant to the objectives. The complete list of standards is presented in figure C.1.

Control Environment

1. The oversight body and management should demonstrate a commitment to integrity and ethical values.

2. The oversight body should oversee the entity's internal control system.

3. Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.

4. Management should demonstrate a commitment to recruit, develop, and retain competent individuals.

5. Management should evaluate performance and hold individuals accountable for their internal control responsibilities.

Risk Assessment

6. Management should define objectives clearly to enable the identification of risks and define risk tolerances.

7. Management should identify, analyze, and respond to risks related to achieving the defined objectives.

8. Management should consider the potential for fraud when identifying, analyzing, and responding to risks.

9. Management should identify, analyze, and respond to significant changes that could impact the internal control system.

Control Activities

10. Management should design control activities to achieve objectives and respond to risks.

11. Management should design the entity's information system and related control activities to achieve objectives and respond to risks.

12. Management should implement control activities through policies.

Information and Communication

13. Management should use quality information to achieve the entity's objectives.

14. Management should internally communicate the necessary quality information to achieve the entity's objectives.

15. Management should externally communicate the necessary quality information to achieve the entity's objectives.

Monitoring

16. Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.

17. Management should remediate identified internal control deficiencies on a timely basis.

Figure C.1. *Components and principles of internal control.*

Source: GAO Standards for Internal Control in the Federal Government.

The inspection team determined that all controls applicable to the Austin clinic aligned with one of the following categories: control environment, control activities, information and communication, and monitoring. When the team identified control activity deficiencies, it 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, violations of legal and regulatory requirements, and abuse could occur during this inspection. The team exercised due diligence in staying alert to any fraud indicators. The OIG did not identify any instances of fraud or potential fraud during this inspection.

Data Reliability

The inspection team generated computer-processed data by using network scanning tools. The results of the scans were provided to the OIT Quality and Compliance Readiness office. The team used industry-standard information system security tools to identify information systems on the VA network and to take snapshots of their configurations, which were used to identify vulnerabilities. In this process, the team was not testing VA data or systems for transactional accuracy. The security tools identified a version of software present on a system, then compared it to the expected version. If the system did not have the current software version, the tool identified it 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 inspection in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation.*

Appendix D: Management Comments

Department of Veterans Affairs Memorandum

Date: May 28, 2021

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

Subj: OIG Draft Report: Inspection of Information Technology Security at the Austin VA Outpatient Clinic Fiscal Year 2020

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

1. The Department of Veterans Affairs (VA) appreciates the opportunity to respond to the Office of Inspector General (OIG) Draft Report, *Inspection of Information Technology Security at the Austin VA Outpatient Clinic, Fiscal Year 2020*. VA concurs with OIG's findings as written.
2. VA is currently developing various projects to correct the items found in the Fiscal Year 2020 audit using the now, near and future timeframes.

The OIG removed point of contact information prior to publication.

(Original signed by)

Dominic Cussat

Attachment

Attachment

Office of Information and Technology Comments on OIG Draft Report, Inspection of Information Technology Security at the Austin VA Outpatient Clinic

OIG Finding 1: The Austin VA Outpatient Clinic Had an Inaccurate Component Inventory and Deficiencies in Vulnerability and Patch Management

Reference: FY20 Austin OPC Inspection Draft Report 3-5-21, Page 9, Paragraph 2

Related OIG Recommendation (1 of 2):

- Recommend that the area manager for the Central Texas Veterans Health Care System implement more effective automated inventory management tools.

OIT Recommendation Response: Concur.

VA is in the process of replacing AEMS/MERS and Maximo with DMLSS, a DoD developed product. The asset inventory that DMLSS will provide includes all procured items and is not limited to devices that are IT related. Additionally, Biomedical Engineering and VHA logistics staff are audited by accreditation agencies and through internal VA processes to ensure all inventory is accurate.

VA utilizes Log Analysis Distributed Data Enterprise Reporting (LADDER), the LADDER application provides a consolidated and flexible interface for the review of MDIA ACL device configuration, ACL interface mapping, and medical device attachment to the VA network for Biomedical staff. Data collection occurs via MS-SQL integration with NCM from the regional SolarWinds instances, UDT on the National Visibility SolarWinds instance, and the Networked Medical Device Database (NMDD). Configuration post-processing is performed to extract ACLs and perform interface mapping.

The LADDER application brings all relevant information together in one location. This tool makes the previously labor-intensive task of reviewing MDIA ACL configurations and medical device location tracking much more efficient, allowing for expeditious remediation. Ultimately, this agentless solution will provide for full visibility of isolated specialized devices, including Medical Devices, special purpose systems (SPS), and research scientific computing devices (RSCD) through device fingerprinting, alerting and displaying, asset discovery and recognition, vulnerability discovery and remediation management.. The Networked Medical Device Database (NMDD) (owned and maintained by Veterans Health Administration (VHA) Office of Healthcare Technology Management (HTM)) and the Special Purpose System Database (owned and maintained by Office of Information Security (OIS) Specialized Device Security Division (SDSD)) provides additional data inputs into LADDER, allowing additional asset management information and categorization. The SMAK (Systems Monitoring and Accountability Knowledge) toolset provides automatic collection of software information inventory for medical devices with a Windows 7 OS and above and Server 2008 R2 and above, but it is not to be used on non-Windows operating systems, older Windows operating systems or any version of Windows Embedded operating systems.

VA has initiated testing and deployment of a specialized device asset management solution under the ECSP Internet of Medical Things (IoMT) project. As a result of the SolarWinds outage, this project already supported provided direct security support (CSOC log behavioral device determination for freezer base stations and traffic identification and security policies Checkpoint/Tempracheck/REES systems) for COVID-19 vaccine administration.

Finally, VA has implemented a Network Access Control System (NAC) that requires any device to be authorized before network communication is allowed. This system will work with the IoMT solution and

other inventory systems to ensure nothing is added to inventory without approval and is accounted for in the system or record.

Short-Term Remediation Milestones:

- Continue execution of the following IoMT project activities:
    - User Acceptance Testing (UAT): completed test plan 3/1/21; testing ongoing
    - Training schedule development for specific target areas
    - CSOC Splunk log data population
    - NUVELO integration discussions/planning activities
    - Qradar integration discussions
    - Mission Impact statement development for Covid Vaccine site implementations
- Continue testing and piloting of IT Asset Management module of ServiceNow, which will migrate the majority of VA Enterprise-wide IT equipment hardware asset management support/ticketing functions from the AEMS/MERS and/or SOARD-Maximo systems to ServiceNow, while logistical functions (property record) will remain with AEMS/MERS and Maximo or DMLSS.
- Continue testing and piloting of the Hardware Asset Management (HAM) and Software Asset Management (SAM) modules within ServiceNow.
- Continue execution of ECSP Project for Special Purpose Systems (SPS) to improve understanding and standardize management of SPS across VA.

Target Maturity Date: 05/30/2021

Near-Term Remediation Milestones:

- Deploy IoMT solution to VAMC Facilities | Target Maturity Date: 9/30/2021
- Final development and adoption of ServiceNow as the host for IT Asset Records | Target Maturity Date: 11/20/2021

Long-Term Remediation Milestones:

- Complete ServiceNow ITAM Module deployment, to include standardization of manufacturers, vendors, warranty support, contact information, and inventory processes for improved oversight on asset delivery and utilization compared to local shelf-stock
- Implement additional functionality, to include asset hand receipt, asset sanitization and decommissioning documentation
- Complete implementation of HAM and SAM modules
- Establish connection between BigFix and ServiceNow to enable hardware and software asset monitoring of non-Windows devices
- Establish DMLSS as the Property Accountability system of record, with a bi-directional information exchange with ServiceNow | Target Maturity Date: 5/20/2022

Related ECSP Projects:

Project Name: FY21-Special Purpose Systems (SPS)

Status: 4%

Expected Completion Date: 09/30/2022

Project Name: FY21-Internet of things Medical Devices (IoMT)

Status: 28%

Expected Completion Date: 10/31/2025

Project Name: FY21-FISMA Containerization

Status: 0%

Expected Completion Date: 11/30/2022

Facility Comments: The OIG scans detected medical devices from the HCS that were outside of the Austin Outpatient Clinic's facility boundary or staff purview. AEMS/MERS is our inventory system of record for hardware. This information feeds into the Corporate Data Warehouse (CDW), which is exported into the IIC portal for verification. The Trusted Agent verified this information for compliance prior to its submission to OIG as evidence.

Related OIG Recommendation (2 of 2):

- Recommend that the area manager for the Central Texas Veterans Health Care System, implement a more effective patch and vulnerability management program that can accurately identify vulnerabilities and enforce patch application.

OIT Recommendation Response: Concur.

Enterprise Response:

- VA maintains a continuous approach to identification and patching (remediation) of security deficiencies. Timeframes for scanning, detection, analysis, criticality, and patching are defined within the associated operational policies and procedures. The ECSP project 104 Improvement of Patch and Vulnerability Management Program identified gaps in lack of procedures and oversight practices. As a result, EVMS has established strategic, tactical, and operational workgroups to define governance, gap analysis, operational process solutions. Additional identification, automation, and compliance-driven patch efforts will be applied to the specific areas mentioned: network infrastructure, database platforms, and web application servers. System level process and procedures are also being identified to address deficiencies in the defined vulnerability management ecosystem.
- Additional identification, automation, and compliance-driven patch efforts will be applied to the specific areas mentioned: network infrastructure, database platforms, and web application servers. System level process and procedures are also being identified to address deficiencies in the defined vulnerability management ecosystem. Additional identification, automation, and compliance-driven remediation efforts could be applied to the specific areas mentioned: network infrastructure, database platforms, and web application servers. These program activities include: addressing gaps in governance or process, implementation guidance, defining roles and responsibilities, ownership, and a focus on standardization of workflows. Projects include: expansion of tools; Information Security Continuous Monitoring tools and enable automated continuous assessment capabilities; the enhancements will provide near real-time data and reduce overhead associated with prioritization, response activity and progress tracking.

- VA Office of Information Security (OIS), Cyber Security Operations Center (CSOC) routinely performs testing for default password configurations throughout the enterprise and the results are distributed for remediation CSOC conducts automated non-credentialed scanning of identified web applications and servers during the quarterly EDS assessment. The agency web application security testing program is primarily performed on a system or application basis. CSOC has expanded this program to include quarterly testing for unsecure web components, common vulnerabilities associated with web services and weak or default passwords and/or configurations throughout the enterprise. CSOC EAS Database Scanning team uses default checks in Oracle and SQL for weak passwords in FISMA policy.
- OIT continues to mature its patch and vulnerability management program, addressing standardization across the enterprise and improving processes for provisioning, testing and deployment of patches, fixes and hardening of systems throughout the VA enterprise network. Strengthening roles and responsibilities.

Corrective Actions/Projects/Initiatives:

- Implementation of Continuous Diagnostic and Mitigation (CDM) 2.0 technology will integrate multiple enterprise data sources into a single dashboard space; promoting greater visibility and strengthening analysis capabilities. This will include Agency-Wide Adaptive Risk Enumeration (AWARE) scoring to allow for prioritization of risk for mitigation activities. Database scanning standardization project identified gaps and provided timelines to ensure inclusion of necessary components. Enhanced IMPERVA scanning capabilities are also being implemented to assist with database scanning management. Web applications vulnerability management standardization project is underway to identify gaps and provide timelines to ensure inclusion of necessary components. Application Control (previously Application Whitelisting) project to address unauthorized and unknown applications is underway.

Remediation Milestones:

- Identify and Improve Patch and Vulnerability Management Program (ECSP 104) is underway
- CDM Dashboard 2.0 production rollout begins May 2021
- Continue Application Control project as a multi-year, phased initiative from 06/2020 to 06/2022
- IMPERVA Database scanning enhancements to continuous monitoring is underway
- ECSP 104, 106, SR1, SR7, SR15 are related or encompassing initiatives

Target Maturity Date: June 30, 2022

Facility Comments: The Austin Outpatient Clinic is not configured on its own isolated network and is a remote site to the main VAMC. The scanning methodology, sample size, or the conclusion reached in this finding may have scanned IP ranges within the Healthcare System network and not limited to the Austin Outpatient Clinic, if OIG is able to provide the vulnerability details of devices scanned, the Austin Outpatient Clinic staff will collaborate with VAMC staff and Enterprise Vulnerability Management Program staff to identify and resolve these issues.

OIG Finding 2 – The Austin VA Outpatient Clinic Had Deficiencies in Media Protection but No Weaknesses Were Found in Other Physical Security Controls:

Reference: FY20 Austin OPC Inspection Draft Report 3-5-21, Page 14, paragraph 2

OIG Recommendation:

- Recommend that the area manager for the Central Texas Veterans Health Care System, ensure compliance with the media protection standard operating procedure for all employees who work with media storage and ensure compliance with marking and sanitization provisions.

OIT Recommendation Response: Concur.

Enterprise Response: OIT concurs with this finding and the corresponding recommendation. Since the scope of this finding is facility-specific, remediation details are provided in the facility comments.

Facility Comments: The area Temple/Waco SOP for Media Protection – MP SOP OIT was completed in 17 April, 2021 to address POAM 1018541125463.

The Area Manager for the Central Texas Veterans Health Care System and the chief biomedical engineer currently distribute this Media Protection SOP to all employees working with media storage, and they ensure compliance with its labeling and sanitization provisions. For all current staff, this action was completed with the updated SOP on April 12, 2021.

OIG Finding 4 – There Were No Weaknesses Found in Access Controls

OIT concurs with this assessment; no response needed as no weaknesses were observed.

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	Mike Bowman and Al Tate, Directors Luis Alicea Cynthia Christian Tom Greenwell Jack Henserling Shawn Hill Francis Hoang George Ibarra Adam Sowells
Other Contributors	Kathy Berrada Michael Soybel

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, Central Texas Veterans 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

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