DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS HEALTH ADMINISTRATION

Inspection of Information Security at the James E. Van Zandt VA Medical Center in Altoona, Pennsylvania

INFORMATION SECURITY INSPECTION | REPORT #22-02960-70 | JUNE 7, 2023

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 (OMB) and applicable National Institute of Standards and Technology (NIST) information security guidelines.[2]

The fiscal year (FY) 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 inspections assess whether VA facilities are meeting federal security requirements. Appendix B presents background information on these requirements. Inspections 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 James E. Van Zandt VA Medical Center (facility) in Altoona, Pennsylvania was meeting federal IT security guidance. The OIG selected the facility because it had not been previously visited as part of the OIG's annual FISMA audit. The inspection scope and methodology are described in appendix C.

This OIG inspection focused on four IT security control areas that apply to local facilities and have been selected based on their levels of risk. The four controls are defined in the Government Accountability Office's (GAO) *Federal Information System Controls Audit Manual* (FISCAM). They include the following:

1. **Configuration management controls** identify and manage security features for all hardware and software components of an information system.[4]
2. **Contingency planning controls** provide reasonable assurance that information resources are protected from unplanned interruptions, minimize risk, and provide

[1] FISMA, Pub. L. No. 113-283, § 128 (2014).

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

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

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

for recovery of critical operations should interruptions occur.[5] 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.
4. **Access controls** provide reasonable assurance that computer resources are restricted to authorized individuals. Theses controls include authorizing and controlling information system components, entering and exiting the facility, and keeping records of those items.[6]

What the Inspection Found

Within configuration management, the inspection team identified deficiencies with component inventory and vulnerability management. The team did not identify deficiencies with contingency planning. The inspection team found that security management had one deficiency with system authorization. Finally, the team identified access control deficiencies in system audit and monitoring and in physical security controls.[7]

Configuration Management Controls Had Two Deficiencies

The facility 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.[8]

[5] GAO, *FISCAM*.

[6] NIST Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*, December 10, 2020.

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

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

The facility did not have accurate inventories, despite the use of automated systems.[9] 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 mostly 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 167 vulnerabilities—66 critical vulnerabilities on about 19 percent of the computers and 101 high-risk vulnerabilities on over 37 percent of the computers—that were previously identified by OIT in a July 2022 scan, 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.[10] The oldest vulnerability was identified on the network in 2017. The OIG also found 64 critical vulnerabilities on about 18 percent of computers and 60 high-risk vulnerabilities on over 37 percent of the computers that would have been detectible by earlier scans, but were not included in OIT's July 2022 scan results.[11] The inspection team could not determine whether these 124 vulnerabilities bypassed detection by VA scanning or were introduced by computers not being vetted for vulnerabilities before being placed on the VA network.[12] Without an effective vulnerability management program, security and functionality problems in software and firmware might not be mitigated, increasing opportunities for exploitation.

Security Management Controls Had One Deficiency

The one security management control deficiency was in system authorization, where management accepts the risk that a system poses to the agency's operations based on implementation of the agreed-upon security controls.[13] The OIG determined that the facility's special-purpose system did not have an authorization to operate.[14] Authorization to operate is management's explicit acceptance that the implementation of security and privacy controls reduce the risk of a system compromise to an acceptable level. The special-purpose system

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

[10] OIT's Authorization Requirements: Standard Operating Procedures, version 1.37 dated June 10, 2022.

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

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

[13] NIST Special Publication 800-53.

[14] The VA's Enterprise Mission Assurance Support Service indicates the special-purpose system "is comprised of operational technology devices/systems that assist, support, and maintain mission capabilities and operations for building safety, healthcare services, security services and other general services functional support areas."

included systems that monitor the distribution of oxygen throughout the hospital, alert facility police of emergencies via panic buttons, control room access, and control facility climate. If the facility's special-purpose system were compromised, the safety of patients, staff members, and visitors would be threatened.

Two Access Controls Had Deficiencies

The facility had security deficiencies in physical access and environmental controls.[15] Concerning physical access deficiencies, the facility did not adequately restrict access to its computer rooms, communication closets, and generators. Specifically,

- the facility did not monitor the distribution of keys that could unlock the computer room and communications closets;
- one of the 27 communication closets did not have a functioning lock mechanism;
- six of the 27 communication closets did not have visitor logs that were being maintained;
- one individual who could use their access card to enter these areas was not listed in the access authorization memos for the computer room; and
- the generators' boiler plant did not have bollards (barriers), there was no fence erected around the generators, and the emergency shut off button for one generator was not secured.

By not adequately restricting access to these areas, the facility is placing IT assets at risk of accidental or intentional destruction.

Further, the team identified the following missing environmental controls in the facility's 27 communication closets; some closets had more than one missing control:

- Twelve communication closets did not have a smoke detector.
- Ten communication closets did not have temperature- and humidity-monitoring controls.
- Nine communication closets did not contain electrical grounding for equipment.
- Nine communication closets did not have fire suppression systems.

Without these safeguards, hazards could damage organizational assets and result in financial loss or harm to veterans.

[15] NIST Special Publication 800-53; VA Directive 6500.

What the OIG Recommended

The OIG recommended that the assistant secretary for information and technology and chief information officer (1) verify and make necessary corrections to the systems' component inventory in VA's Enterprise Mission Assurance Support Service, (2) improve vulnerability management processes to ensure system changes occur within organization timelines, and (3) develop and approve an authorization to operate for the facility's special-purpose system. 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 facility director validate that appropriate physical and environmental security measures are implemented and functioning as intended.[16]

VA Comments and OIG Response

The assistant secretary for information and technology and chief information officer concurred with recommendations 2, 3, and 4; however, he did not concur with recommendation 1. Regarding recommendation 1, the assistant secretary reported OIT has an automated assignment process to ensure assets are identified by the correct boundaries. The assistant secretary stated that the discrepancy in numbers is a direct result of OIT's interpretation of language used in the OIG request process. The OIG identified approximately 2,500 devices on the facility's network as compared to approximately only 1,450 devices identified by the component inventory in VA's Enterprise Mission Assurance Support Service. The assistant secretary committed to seeking "clarifying evidence request language" going forward, but did not identify the specific language that resulted in interpretation questions or how it raised interpretation questions. Further, OIT did not submit additional evidence to resolve this discrepancy in the numbers. The OIG therefore stands by its conclusion.

The assistant secretary concurred with recommendation 2 but stated that VA consistently maintains a 90 percent or greater management rate of critical vulnerabilities across the enterprise. However, VA did not provide evidence that would allow the OIG to validate this assertion. In fact, OIT's March 2023 response indicated that only 69 percent of the critical and high-risk vulnerabilities had remediations completed, while the remaining vulnerabilities were awaiting updates or had corresponding plans of actions and milestones.

The assistant secretary concurred with recommendations 3 and 4 and reported that VA will ensure special purpose systems have formal authorities to operate, and the Electronic Health Record Modernization project will remediate all physical and environmental security measure

[16] The recommendation addressed to the medical center director is applicable to anyone in an acting status or performing the delegable duties of the position.

controls in FY 2026. The assistant secretary reported that corrective actions for recommendations 3 and 4 are in progress and provided estimated completion dates.

The planned corrective actions are responsive to the intent of recommendations 2 through 4. The OIG will keep the recommendations open until OIT's proposed changes are implemented and OIT will report quarterly on its progress toward implementation. The full text of the assistant secretary's response is included in appendix D.

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 of 2014
FY	fiscal year
GAO	Government Accountability Office
IT	information technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information and Technology
OMB	Office of Management and Budget

Introduction

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.[17] The FISMA audit is conducted in accordance with guidelines issued by the Office of Management and Budget (OMB) and applicable National Institute of Standards and Technology (NIST) information security guidelines.[18]

In 2020, the OIG started an information security inspection program. These inspections assess whether VA facilities are meeting federal IT security requirements that protect systems and data from unauthorized access, use, modification, or destruction.[19] They are typically conducted at selected facilities that have not been assessed in the sample for the annual FISMA audit or at facilities that previously performed poorly. Inspections provide recommendations to VA on enhancing information security oversight at local facilities.[20] Appendix C provides more detail on the inspection scope and methodology. The OIG conducted this inspection to determine whether the James E. Van Zandt VA Medical Center (facility) was meeting those requirements. The OIG selected this facility because it had not been previously visited as part of the annual FISMA audit. Although the findings and recommendations in this report are specific to this facility, leaders at other facilities across VA could benefit from reviewing this information and considering these recommendations.

Security Controls

Both the OMB and 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.[21]

---

[17] Federal Information Security Modernization Act of 2014 (FISMA), Pub. L. No. 113-283, § 128 (2014). Appendix A details the recommendations from the FY 2021 FISMA audit.

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

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

[20] 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.

[21] OMB, "Security of Federal Automated Information Resources," app. III in OMB Circular A-130, July 28, 2016; NIST Special Publication 800-53.

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

The OIG's 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.

Table 1. Security Controls Evaluated by the OIG

Control area	Purpose	Examples evaluated
Configuration management	Identify and manage security features for all hardware and software components of an information system	Component inventory, baseline configurations, configuration settings, change management, vulnerability management, and flaw remediation
Contingency planning	Provide reasonable assurance that information resources are protected and risk of unplanned interruptions is minimized, as well as provide for recovery of critical operations should interruptions occur	Continuity of operations, contingency planning, disaster recovery, environmental, and maintenance
Security management	Establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of the procedures	Risk management, assessment, authorization, and monitoring
Access	Provide reasonable assurance that computer resources are restricted to authorized individuals	Access, identification, authentication, audit, and accountability, including related physical and environmental security controls, such as authorization, visitors, and monitoring delivery and removal

Source: VA OIG analysis.

[22] VA Handbook 6500, *Risk Management Framework for VA Information Systems: VA Information Security Program*, February 24, 2021.

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.

Office of Information and Technology Structure and Responsibilities

The assistant secretary for information and technology and chief information officer leads the Office of Information and Technology (OIT). According to VA, OIT delivers available, adaptable, secure, and cost-effective technology services to VA and acts as a steward for VA's IT assets and resources. 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 it, End User Operations provides onsite and remote support to IT customers across all VA administrations and special program offices, including direct support of over 340,000 VA employees and thousands of contractors who are issued government-furnished IT equipment and access. The End User Operations office provisions computing devices; conducts new facility activations; performs moves, adds, and changes; executes local system implementations; and engages VA's customers across the nation to meet IT support needs. OIT assigns dedicated End User Operations personnel to the facility. 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. The hierarchy is shown in figure 1.

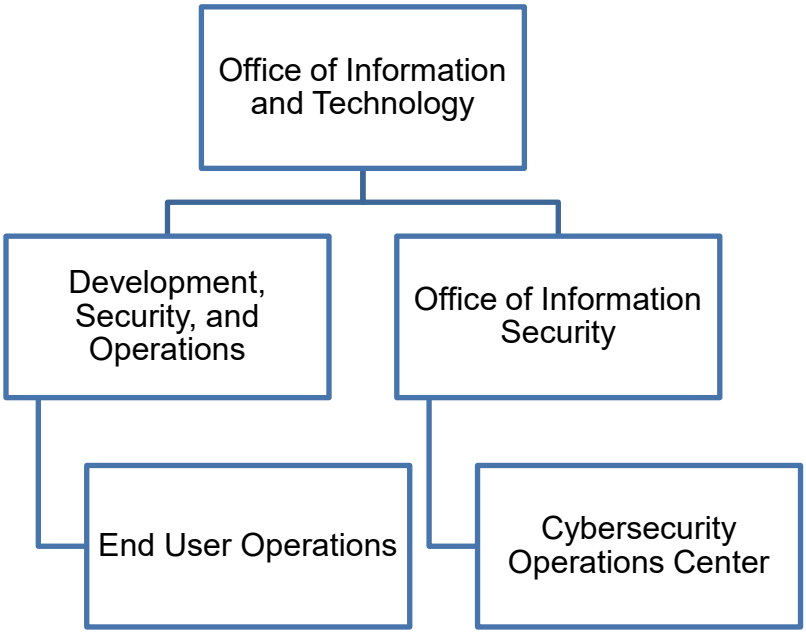

Figure 1. *Organizational structure of Office of Information and Technology entities relevant to this inspection.*
Source: VA OIG analysis.

Results of Previous Projects

As previously mentioned, the OIG issues annual reports on VA's information security program. The FISMA audit is conducted in accordance with guidelines issued by OMB and applicable NIST information security guidelines.[23] The fiscal year (FY) 2021 FISMA audit, conducted by CliftonLarsonAllen LLP, an independent public accounting firm, evaluated 50 major applications and general support systems hosted at 24 VA facilities, including the testing of selected management, technical, and operational controls outlined by NIST.[24] 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.[25] Repeat recommendations included addressing deficiencies in configuration management, contingency planning, security management, and access controls.

A statement prepared by the Government Accountability Office (GAO) for a House Veterans' Affairs subcommittee hearing in November 2019 said VA was one of the federal agencies that continued to have a deficient information security program.[26] According to GAO, as VA secured and modernized its information systems, it faced several security challenges including

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

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."[27]

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

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

[25] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2021.* Appendix B presents information about FISMA and other federal criteria and standards discussed in this report.

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

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

James E. Van Zandt VA Medical Center

The facility is part of the VA Altoona Healthcare System in Pennsylvania. The facility saw 26,301 unique outpatients in FY 2021. It also houses 11 acute care beds and 40 community living center beds.[28] The facility had 1,116 full-time employees and a budget of $190 million for FY 2022.

Figure 2. *James E. Van Zandt VA Medical Center.*

Source: James E. Van Zandt VA Medical Center Visual Information Specialist Evan Hinkley, September 1, 2021.

[28] The community living center beds are used for nursing home services provided by VA.

Results and Recommendations

I. Configuration Management Controls

According to the GAO's *Federal Information System Controls Audit Manual* (FISCAM), configuration management involves identifying and managing security features for all hardware, software, and firmware components of an information system at a given point and systematically controlling changes to that configuration during the system's life cycle.[29] The inspection team reviewed and evaluated the 12 configuration management controls drawn from NIST criteria for VA-hosted systems at the facility 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.[30] VA should first establish an accurate component inventory to identify all devices on the network.[31] The component inventory affects the success of other controls, such as vulnerability and patch management. According to the configuration management standard operating procedure, OIT's Cybersecurity Operations Center identifies and reports on threats and vulnerabilities, and OIT's patch and vulnerability team develops procedures to remediate these issues, which can include applying patches. This process helps to secure devices from attack.[32]

Finding 1: The Facility Had Two Configuration Management Control Deficiencies

The OIG found that the facility had inaccuracies in the component inventory and weaknesses in vulnerability management. To assess these configuration management controls, the inspection team interviewed the system owner, information system security officers, system stewards, and personnel from the facility's Systems Program Management office. The team observed system change management processes; reviewed local policies, procedures, and inventory lists; and scanned the facility's network to identify devices. The team compared the devices found on the network with the device inventories found in the Enterprise Mission Assurance Support Service, 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.[33]

---

[29] GAO, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G, February 2009.
[30] GAO, *FISCAM.*
[31] GAO, *FISCAM.*
[32] VA Handbook 6500.
[33] See appendix C for additional information about the inspection's scope and methodology.

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.[34] A comprehensive view of the components improves a security program by identifying what needs to be managed and secured. The OIG identified approximately 2,500 devices on the facility's network. However, the component inventory in VA's Enterprise Mission Assurance Support Service identified approximately only 1,450 devices.[35] Since VA's Enterprise Mission Assurance Support Service is used for the development of facility system security and privacy plans, VA has no assurance that corresponding system security and privacy plans have identified the appropriate security controls for all components at the facility without an accurate inventory of network devices.

Vulnerability Management

Prior FISMA audits repeatedly found deficiencies in VA's vulnerability assessments, and the OIG identified vulnerabilities at the facility consistent with those findings. According to 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."[36] 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 routinely and randomly, or when new vulnerabilities are identified and reported.

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 10.0, whereas high-risk vulnerabilities have a score between 7.0 and 8.9.

OIT conducts periodic independent scans of all VA-owned systems. 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

[34] GAO, *FISCAM.*

[35] Enterprise Mission Assurance Support Service 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.

[36] GAO, *FISCAM.*

mitigation or remediation efforts for each deficiency identified from the scan and provides evidence that the deficiencies have been mitigated within established deadlines, based on severity of the vulnerability: 30 days for critical vulnerabilities and 60 days for high-risk vulnerabilities.[37]

The OIG determined that OIT's vulnerability identification process and scans were mostly effective; however, the process to remediate identified vulnerabilities needs improvement. The inspection team compared OIT's vulnerability scan results with scans the inspection team conducted from July 18 through 21, 2022. OIT and the team used the same vulnerability-scanning tools. The inspection team identified 167 vulnerabilities, including 66 critical vulnerabilities on about 19 percent of the computers and 101 high-risk vulnerabilities on over 37 percent of the computers that were previously identified by OIT but were not mitigated as quickly as expected. The oldest vulnerability was identified on the network in 2017.

The OIG also found 64 critical vulnerabilities on 18 percent of computers and 60 high-risk vulnerabilities on 37 percent of computers that would have been detectible by earlier scans but were not included in OIT's July 2022 scan results.[38] The inspection team could not determine whether these 124 vulnerabilities bypassed detection by VA scanning or were introduced by computers not being vetted for vulnerabilities before being placed on the VA network.[39] Similarly, the prior FISMA audit found that OIT "did not have a complete inventory of all vulnerabilities present on locally hosted systems."[40] Without an effective vulnerability 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 facility did not have accurate component inventories in its security program, a problem that could lead to devices not being effectively managed and secured. The vulnerability management controls used by VA and the facility were ineffective as they did not ensure a comprehensive patch management process will meet organizational timelines. 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.

[37] OIT's Authorization Requirements: Standard Operating Procedures, version 1.37 dated June 10, 2022.

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

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

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

Recommendations 1–2

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

1. Verify and make necessary corrections to the systems' component inventory in the VA's Enterprise Mission Assurance Support Service.
2. Improve vulnerability management processes to ensure system changes occur within organization timelines.

VA Management Comments

The assistant secretary for information and technology and chief information officer did not concur with recommendation 1. The assistant secretary reported OIT has an automated assignment process to ensure assets are identified by the correct authorization boundaries.[41] The assistant secretary stated that the discrepancy in numbers is a direct result of OIT's interpretation of language used in the OIG request process. The assistant secretary also stated that OIT will seek clarification on future OIG information requests.

The assistant secretary concurred with recommendation 2 and reported that VA consistently maintains a 90 percent or greater management rate of critical vulnerabilities across the enterprise. Further, the assistant secretary stated that VA will follow up on remaining pending or status update vulnerability items to ensure those vulnerabilities are addressed to a compliant state.

OIG Response

Regarding the assistant secretary's nonconcurrence with recommendation 1, OIT's response did not include additional evidence that would prompt the OIG to reconsider its conclusion. The OIG identified approximately 2,500 devices on the facility's network as compared to approximately only 1,450 devices identified by the component inventory in VA's Enterprise Mission Assurance Support Service. Further, VA did not identify the language that was the subject of the interpretation issues, or what about the language caused those concerns. The OIG's results were provided to OIT and discussed with OIT leaders throughout the inspection. OIT personnel did not raise any concerns related to the inventory issue prior to their written response to the draft report.

The assistant secretary provided corrective actions for recommendation 2 that are responsive to the intent of the recommendation. Despite concurring with recommendation 2, the assistant secretary stated that VA consistently maintains a 90 percent or greater management rate of critical vulnerabilities across the enterprise. However, VA did not provide evidence that would

[41] The Altoona Healthcare System has three authorization boundaries, including: General Support Systems, Special Purpose Systems, and Medical Systems.

allow the OIG to validate this assertion. OIT's March 2023 response only showed that only 69 percent of the critical and high-risk vulnerabilities had remediations completed, while the remaining vulnerabilities were awaiting updates or had corresponding plans of actions and milestones. When OIT provides documentation to support that patching has remediated the vulnerabilities or that compensating controls are in place to reduce the risk of exploitation of the vulnerabilities, the OIG will close recommendation 2. The full text of the assistant secretary's response is included in appendix D.

II. Contingency Planning Controls

According to GAO's FISCAM, "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."[42] To determine whether recovery plans will work as intended, they should be tested periodically in disaster simulation exercises.[43] 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."[44] Although often referred to as disaster recovery or contingency plans, controls to ensure service continuity should address the entire range of potential disruptions.[45] These may include minor interruptions, such as temporary power failures, as well as fires, natural disasters, and terrorism, which would require reestablishing operations at a remote location. To determine if the facility met federal guidance and VA requirements, the inspection team evaluated five contingency planning controls.[46]

Finding 2: The Facility Had No Contingency Planning Control Deficiencies

To assess contingency planning controls, the inspection team interviewed the area manager, the information system security officer, members of OIT's Office of Development, Security and Operations, and facility management. The team also reviewed local policies and procedures.

The OIG found that VA's policies and procedures addressed control criteria such as identifying critical operations and performing preventive maintenance. The team verified that the site's information system contingency plan established comprehensive procedures to recover the facility's IT operations quickly and effectively following a service disruption. Furthermore, the facility conducted contingency training, testing, and recovery exercises in accordance with policies. The team did not identify deficiencies in contingency planning controls. Accordingly, the OIG did not make any recommendations for improvement.

[42] GAO, *FISCAM*.

[43] GAO, *FISCAM*.

[44] FISMA.

[45] GAO, *FISCAM.*

[46] The five contingency controls evaluated include continuity of operations, contingency planning, disaster recovery, environmental, and maintenance.

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 security procedures. The inspection team evaluated processes related to the implementation of a security management program.[47]

Finding 3: The Facility Had One Security Management Control Deficiency

To assess security controls, the inspection team reviewed local security management policies, standard operating procedures, and applicable VA policies. These included documentation from the Enterprise Mission Assurance Support Service. Among the topics reviewed were the handling of external media and system authorization. The team interviewed information system security officers, local administrators, contracting officer's representatives, privacy officers, and system stewards. The team also conducted a walk-through of the facility. The OIG found one security management control deficiency in connection with the system authorization process for a special-purpose system.

System Authorization

The OIG determined that the facility's special-purpose system did not have an authorization to operate because it had not cleared the NIST risk management framework process.[48] Authorization to operate is management's explicit acceptance of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security and privacy controls.[49] The special-purpose system included components that monitor the distribution of oxygen throughout the hospital, alert facility police of emergencies via panic buttons, control room access, and control the facility's climate.

Without an authorization to operate, facility managers do not have assurance that implemented security and privacy controls reduce the risk of a system compromise to an acceptable level. If the facility's special-purpose system were compromised, the safety of patients, staff members, and visitors would be threatened.

[47] FISCAM critical elements for security management are listed in appendix B.

[48] VA's Enterprise Mission Assurance Support Service indicates the special-purpose system "is comprised of operational technology devices/systems that assist, support, and maintain mission capabilities and operations for building safety, healthcare services, security services and other general services functional support areas."

[49] NIST Special Publication 800-53.

Finding 3 Conclusion

Security management controls at the facility did not ensure systems included controls that reduced the risk of loss of confidentiality, integrity, and availability to a level that management considers acceptable. Without effective security 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.

Recommendation 3

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

3. Develop and approve an authorization to operate for the special-purpose system.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendation 3 and reported that VA will ensure that special purpose systems have formal authorities to operate. The estimated completion date for this corrective action is January 2025.

OIG Response

The planned corrective actions are responsive to the intent of the recommendation. Given the complexity of the special purpose system environment, the estimated completion date of January 2025 is acceptable.[50] The OIG will keep the recommendation open until OIT's proposed changes are implemented, and OIT will report quarterly on its progress toward implementation. The full text of the assistant secretary's response is included in appendix D.

[50] The special purpose system environment is complex as it contains a wide variety of components with different owners. These include police systems including camera systems, facility maintenance systems such as heating, ventilation, and air conditioning systems, and patient care systems including TeleSitter which is used to remotely observe patients.

IV. Access Controls

Previous FISMA reports have repeatedly identified access controls as a nationwide issue for VA. Access controls, including boundary protections, sensitive system resources, physical security, and audit and monitoring controls provide reasonable assurance that computer resources are restricted to authorized individuals. Access also includes physical and environmental controls associated with physical security, such as authorization, visitors, monitoring, delivery, and removal. Identification, authentication, and authorization controls ensure that users have the proper access, and that access is restricted to authorized individuals. At the facility, the inspection team reviewed six critical access control elements.[51]

Finding 4: The Facility Had Two Access Control Deficiencies

To evaluate the facility'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 facility; and analyzed visitor logs.[52]

The OIG found these issues with access controls:

- The facility did not adequately restrict access to its computer rooms, communication closets, and generators.
- The facility did not implement controls for electrical grounding of equipment, environmental controls for temperature and humidity monitoring, and fire detection and suppression within certain computer rooms and communication closets.

Physical Controls

Physical access is the process used to restrict individuals' ability to enter computer rooms and communication closets to protect computer resources from intentional or unintentional loss or impairment.[53] The OIG found that the facility did not adequately restrict access to its computer rooms, communication closets, and generators, as described in the following list:

- The facility did not monitor the distribution of keys that could unlock the computer room and communications closets.
- One of the 27 communication closets did not have a functioning lock mechanism.
- Six of the 27 communication closets did not have visitor logs that were being maintained.

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

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

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

- One individual who could use their access card to enter these areas was not listed in the access authorization memos for the computer room.
- The generators' boiler plant did not have bollards (barriers), there was no fence erected around the generators, and the emergency shut off button for one generator was not secured.

By not adequately restricting access to these areas, the facility is placing IT assets at risk of accidental or intentional damage or destruction.

Environmental Controls

The facility had several deficiencies in IT environment controls that protect computer resources from harm. The OIG found the following deficiencies:

- Twelve communication closets did not have a smoke detector.
- Ten communication closets did not have temperature- and humidity-monitoring controls.
- Nine communication closets did not contain electrical grounding for equipment.
- Nine communication closets did not have fire suppression systems.

Without these environmental safeguards, organizational assets could be damaged by electrical surges, water, or fire, resulting in financial loss or harm to veterans.

Finding 4 Conclusion

The facility's access controls did not ensure that computer resources were protected from theft and intentional or accidental damage. If the deficiencies are not corrected, the facility may not be able to properly respond, may lose public trust, and may incur costs to recover from a loss of data or destruction of computer resources.

Recommendation 4

The OIG made one recommendation to the facility director:

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

VA Management Comments

The assistant secretary responded on behalf of the facility director and concurred with recommendation 4, reporting that the Altoona VA Medical Center Electronic Health Record Modernization project will remediate all physical and environmental security measure controls in

FY 2026. The assistant secretary requested the removal or closure of recommendation 4 deficiencies related to access to IT closets and visitor logs.

OIG Response

The planned corrective actions are responsive to the intent of the recommendation. The assistant secretary provided adequate evidence demonstrating actions had been taken to address some issues the OIG identified related to access to IT closets and visitor logs and requested the removal or closure of the recommendation. The OIG acknowledges these particular issues have been remediated; however, the OIG will keep the recommendation open until OIT's proposed changes are implemented to address all physical and environmental security issues and OIT will report quarterly on its progress toward implementation. The OIG also acknowledges that some physical and environmental security measures will not be remediated until work related to the Electronic Health Record Modernization project is completed at the facility. The full text of the assistant secretary's response is included in appendix D.

Appendix A: FISMA Audit for FY 2021 Report Recommendations

In the FISMA audit for FY 2021, CliftonLarsonAllen LLP made 26 recommendations, all of which 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 facility. 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.
12. Implement a more effective patch and vulnerability management program to address security deficiencies identified during 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.[54]
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.
22. Implement improved safeguards to identify and prevent unauthorized vulnerability scans on VA networks.

[54] Credentialed vulnerability assessments are vulnerability scans performed using a user account and password.

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

GAO developed FISCAM to provide auditors and information system control specialists with 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 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.[55] 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

[55] 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 management 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 management.

- **Implement security awareness and personnel policies** that provide training for new employees, contractors, and users; periodic refresher training; and distribution of security policies detailing rules and expected behaviors. This element also addresses hiring, transfers, terminations, and performance for employees, contractors, and users. Examples of controls in this area are security awareness training, rules of behavior, position categorization, personnel policies, personnel screening, termination, transfer, access agreements, third-party personnel security, and personnel sanctions.
- **Monitor the program** to ensure that policies and controls effectively reduce risk on an ongoing basis. Effective monitoring involves testing controls to evaluate and determine whether they are appropriately designed and operating effectively. Examples of these controls are security assessments, continuous monitoring, privacy impact assessments, and vulnerability scanning.
- **Remediate information security weaknesses** when they are identified, which involves reassessment of related risks, applying appropriate corrective actions, and 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.[56]

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

[56] 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 authorized users can do. These controls grant or restrict user, service, or device access to various resources based on the identity of the user, service, or device.

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.[57]

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.

[57] 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 inspection team conducted its work from July 2022 through January 2023. 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 facility and systems for security compliance. Additionally, the team interviewed VA personnel responsible for the facility's IT security, 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 inspection team determined that internal controls were significant to the inspection objectives. The overall scope of IT security inspections is the evaluation of general security and application controls that support VA's programs and operations. According to the risk management framework for VA information systems, the information security program is the foundation for VA's information security and privacy program and practices. The framework is documented in VA Handbook 6500.

The team used the GAO's FISCAM as a template to plan for inspections. When planning for this review, the team identified potential information system controls that would significantly affect the review. Specifically, the team used FISCAM appendix II as a guide to help develop evidence requests and interview questions for James E. Van Zandt VAMC 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 are included 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 James E. Van Zandt VAMC 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 audit objectives, could occur during this inspection. The team exercised due diligence in staying alert to any fraud indicators. The OIG did not identify any instances of fraud or potential fraud during this inspection.

Data Reliability

The inspection team generated computer-processed data by using network scanning tools. The results of the scans were provided to the OIT Quality 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 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 review in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation.*

Appendix D: VA Management Comments

Department of Veterans Affairs Memorandum

Date: March 12, 2023

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

Subj: Office of Inspector General Draft Report: Inspection of Information Technology Security at the James E. Van Zandt Medical Center in Altoona, Pennsylvania (VIEWS 09380068)

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 Security at the James E. Van Zandt Medical Center in Altoona, Pennsylvania (Project Number 2022-02960-AE-0118).

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

The OIG removed point of contact information prior to publication.

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 at the
James E. Van Zandt Medical Center in Altoona, Pennsylvania (VIEWS 09380068)

Recommendation 1: Verify and make necessary corrections to the systems' component inventory in the VA's Enterprise Mission Assurance Support Service.

Comments: Non-Concur.

The Department of Veterans Affairs (VA) Office of Information and Technology (OIT) has an automated assignment process to ensure assets are identified by the correct boundaries. The discrepancy in numbers is a direct result of the interpretation of language used in the Office of Inspector General (OIG) request process. OIT will seek clarifying evidence request language for future audits. VA identified assets when all system boundaries were included. Network connected assets are managed by the VA vulnerability management process with the accountable system owners.

Recommendation 2: Improve vulnerability management processes to ensure system changes occur within organization timelines.

Comments: Concur.

OIT's overall patch and vulnerability compliance percentages provide evidence that VA has implemented, and is managing, an effective vulnerability management and flaw remediation program, aligned with VA and industry standards. VA consistently maintains a 90% or greater management rate of critical vulnerabilities across the enterprise. VA's latest analysis of OIG's scan results for the Altoona VA Medical Center displays 99.31% policy compliance. VA will follow up on remaining pending or status update vulnerability items to ensure those vulnerabilities are addressed to a compliant state.

Expected Completion Date: May 1, 2023.

Recommendation 3: Develop and approve an authorization to operate for the special-purpose system.

Comments: Concur.

VA OIT will ensure that special purpose systems have formal authorities to operate.

Expected Completion Date: January 31, 2025

Recommendation 4: Validate that appropriate physical and environmental security measures are implemented and functioning as intended.

Comments: Concur.

The Altoona VA Medical Center Electronic Health Record Modernization project will remediate all physical and environmental security measures controls in fiscal year (FY) 2026. VA OIT awarded and planned a project to remediate the generators by FY 2024.

The Altoona VA Medical Center remediated the following items:

- Information technology (IT) closets.
- Visitor logs.

Expected Completion Date: September 30, 2024, and September 30, 2026.

VA OIT requests removal or closure of recommendation 4 deficiencies related to access to IT closets and visitor logs.

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	Eldridge Harding Clifford Stoddard

Report Distribution

VA Distribution

Office of the Secretary
Veterans Benefits Administration
Veterans Health Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel
Office of Acquisition, Logistics, and Construction
Board of Veterans' Appeals

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Accountability
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget
US Senate: Robert Casey Jr., John Fetterman
US House of Representatives: John Joyce, Scott Perry, Guy Reschenthaler, Glenn "GT" Thompson

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