DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS HEALTH ADMINISTRATION

Inspection of Information Technology Security at the Alexandria VA Medical Center in Louisiana

INFORMATION TECHNOLOGY INSPECTION

REPORT #22-00971-217

SEPTEMBER 22, 2022

MISSION

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

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

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

www.va.gov/oig/hotline

1-800-488-8244

Executive Summary

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

The fiscal year 2021 FISMA audit indicated that VA continues to face significant challenges meeting the law's requirements. The audit made 26 recommendations to VA. Repeat recommendations included addressing deficiencies in configuration management, contingency planning, security management, and access controls.[3] Appendix A details these recommendations.

In 2020, the OIG also started an IT security inspection program. These IT inspections assess whether VA facilities are meeting federal security requirements related to four control areas selected based on their levels of risk.[4] They are typically conducted at selected facilities that have not been assessed in the sample for the annual audit or at facilities that previously performed poorly.

The OIG conducted this inspection to determine whether the Alexandria VA Medical Center (VAMC) in Louisiana was meeting federal security guidance. The OIG selected the Alexandria VAMC because it had not been previously visited as part of the annual FISMA audit. The inspection scope and methodology are described in appendix C.

The OIG's inspections are focused on the following four security control areas:

1. **Configuration management controls** identify and manage security features for all hardware and software components of an information system.[5]
2. **Contingency planning controls** provide reasonable assurance that information resources are protected from unplanned interruptions, minimize risk, and provide

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

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

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

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

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

for recovery of critical operations should interruptions occur.[6] Contingency planning also includes physical and environmental controls, such as fire protection, water damage protection, and emergency power and lighting.

3. **Security management controls** "establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of the procedures."[7]
4. **Access controls** provide reasonable assurance that computer resources are restricted to authorized individuals. Access also includes physical and environmental controls associated with physical security, such as authorization, visitors, monitoring, delivery, and removal.[8]

What the Inspection Found

The OIG identified deficiencies with configuration management, security management, and access controls. The inspection team did not identify deficiencies with contingency planning controls.

Configuration Management Controls Had Four Deficiencies

The Alexandria VAMC had security deficiencies in the following configuration management controls:

- Component inventory is a descriptive record of IT assets in an organization down to the system level.
- Vulnerability management is the process by which the Office of Information and Technology (OIT) identifies, classifies, and reduces weaknesses.
- Flaw remediation is how organizations correct software defects and often includes system updates, such as security patches.[9]
- Unsupported system components occur when developers no longer update their products.[10]

[6] GAO, *FISCAM*.

[7] GAO, *FISCAM*.

[8] GAO, *FISCAM*.

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

[10] NIST Special Publication 800-53.

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

The OIG determined that OIT's process to remediate identified vulnerabilities needs improvement. OIT scans for vulnerabilities routinely, randomly, and when new vulnerabilities are identified and reported. Although the inspection team and OIT used the same vulnerability-scanning tools, OIT did not detect all the vulnerabilities the team found. Some of the vulnerabilities were present on multiple devices. The inspection team identified 33 vulnerabilities—17 critical vulnerabilities on 8 percent of the devices and 16 high-risk vulnerabilities on 29 percent of the devices—which were not mitigated within the time frames established by OIT. The OIG also found five critical vulnerabilities and three high-risk vulnerabilities that OIT did not detect. While the agency is aware of many of the vulnerabilities, the plans of actions and milestones did not always list a remediation.[11] Overall, the OIG identified critical and high-risk vulnerabilities on 37 percent of the devices at Alexandria VAMC.

Despite VA's significant patch management measures, the OIG inspection team identified several devices that were missing patches. Several devices with critical and high-risk vulnerabilities had patches available that were not applied. Some had been on the network for as long as three years after initial discovery by VA. Without these controls, VA may be placing critical systems at unnecessary risk of unauthorized access, alteration, or destruction.

Almost 12 percent of the Alexandria VAMC network switches used operating systems that were no longer supported by the vendor. Consequently, these devices will not receive maintenance or vulnerability support, which can result in an opportunity for adversaries to exploit weaknesses in the components.[12] Network devices and IT systems are an organization's most critical infrastructure. Upgrading is not just a defensive strategy but a proactive one that protects the stability of the network.

Security Management Was Deficient in Control Assessment

The team identified one security management deficiency in control assessment, which involves evaluating the system and its operational environment to determine whether controls are

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

[12] NIST Special Publication 800-53.

implemented correctly, operating as intended, and producing the desired outcome for security and privacy requirements.[13]

The Alexandria VAMC did not have an authorization to operate for the video surveillance system, a requirement for systems with an external connection. Control assessments are part of an authorization to operate. The lack of control assessment led to a myriad of other deficiencies, such as unsupported network infrastructure equipment, a vulnerable network operating system, and improperly protected credentials. The system was operated by facility maintenance personnel who are not part of OIT. Without measures in place to assess controls, vulnerabilities existed that would impact the integrity and protection of the video surveillance system.

Four Access Controls Had Deficiencies

The Alexandria VAMC had four deficiencies in access controls, which provide reasonable assurance that computer resources are restricted to authorized individuals and ensure users have the proper access and are uniquely identified. The following access controls were deficient:

- Equipment installation ensures equipment is installed according to established standards, reducing the risk of damage.
- Emergency power provides near-instantaneous protection from unanticipated power interruptions and protects equipment where unexpected power disruption could cause injuries, fatalities, mission or business disruption, or loss of information.
- Identification and authentication controls distinguish one user from another and establish the validity of a user's claimed identity.
- Physical access involves restricting access to computer resources and protecting them from intentional or unintentional loss or impairment.[14]

The OIG found the Alexandria VAMC did not have properly installed network infrastructure equipment. The team identified several instances of network equipment not mounted to equipment racks. Consequently, the devices are susceptible to fall damage, which has the potential to interrupt availability of information for the portions of the network served by that equipment. Further, some of the equipment is stacked on top of each other, which does not allow for proper cooling and increases the chance of equipment failure due to overheating.

During a routine walk-through, the inspection team found an uninterruptible power supply that had completely failed and a second with a failed battery that supported the facility's network infrastructure. An uninterruptible power supply is an electrical system or mechanism that

[13] NIST Special Publication 800-53.

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

provides emergency power when there is a failure of the main power source. OIT personnel responsible for maintenance of the network equipment were not conducting routine maintenance that would have detected the failed uninterruptible power supply and battery and would have resulted in replacement. Without operational uninterruptible power supplies, the infrastructure equipment will not function during power fluctuations or outages, which would interrupt data flow and disrupt access to network resources.

The OIG also identified deficiencies in identification and authentication—specifically, databases that do not enforce password changes in accordance with VA information security policy. The inspection team's scan results also indicated that the VAMC servers allow local credentials that rely on weak, single-factor authentication to provide system access. Further, the passwords were not set to expire on servers in accordance with VA policy. According to OIT, the weak password settings are required for older applications to prevent them from "breaking." However, OIT also acknowledged that deviations from the policy were not approved. Weak password controls expose organizations to a greater risk of compromise. Once compromised, a local database account could be used for unauthorized disclosure or modification of personal health information.

Finally, the physical access controls system used for the Alexandria VAMC data center and core switch room is ineffective. It uses an outdated operating system and did not produce audit logs, contrary to VA policy. The site is required to monitor physical access where information systems reside and review access logs quarterly. The lack of logging capability makes it difficult to identify potential security incidents and suspicious activities, such as access outside of normal work hours, access for an unusual length of time, or out-of-sequence access. The outdated operating system also puts the overall system at a higher security risk, makes it more susceptible to computer viruses, and is difficult to replace, thereby creating a potential single point of failure to the datacenter and core switch room. The facility does have a centralized, campus-wide physical access control system; however, it is not currently being used for the datacenter and core switch room.

What the OIG Recommended

The OIG made six recommendations to the assistant secretary for information and technology and chief information officer: implement a more effective process to maintain consistent inventory information for all network segments, improve the vulnerability and flaw remediation program to accurately identify vulnerabilities and enforce flaw remediation, implement effective configuration control processes that ensure network devices maintain vendor support, ensure proper installation of network equipment, ensure routine maintenance is conducted on uninterruptible power supplies, and implement database authentication processes that comply with VA security requirements. The OIG made these recommendations to the assistant secretary because they are related to enterprise-wide IT security issues similar to those identified on

previous FISMA audits and IT security reviews. The OIG also made two recommendations to the Alexandria VAMC director: performing security control assessments for the video surveillance system seeking an authorization to operate and implementing a physical access control security system that is supportable and can meet VA security standards.

VA Comments and OIG Response

The assistant secretary for information and technology and chief information officer provided comments for the Alexandria VAMC. The assistant secretary concurred with all eight recommendations. The assistant secretary requested recommendations 1, 2, 6, and 7 be closed due to corrective actions he said were completed. The assistant secretary provided responsive actions plans for the recommendations. Based on the responsive actions plans provided by the assistant secretary, the OIG considers recommendations 1, 2, 6, and 7 closed. The OIG will monitor implementation of planned actions and close the remaining open recommendations when VA provides sufficient evidence demonstrating progress in addressing the recommendations and the issues identified. The full text of the response from the assistant secretary is included in appendix D.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluation

Contents

Abbreviations

FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Modernization Act
GAO	Government Accountability Office
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information and Technology
VAMC	VA medical center

Introduction

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

FISMA was established, in part, to improve oversight of federal agency information security programs. The law requires VA to develop, document, and implement an agencywide information security and risk management program. FISMA also requires the chief information officers and other senior agency officials to report annually on the effectiveness of the agency's information security program. In addition, FISMA states that inspectors general are required to conduct annual independent evaluations of their respective agencies' information security programs. To determine compliance with FISMA, the OIG contracts with an independent public accounting firm that conducts an annual audit of VA's information security program and practices.[16]

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

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

[16] See appendix A for a list of recommendations resulting from the most recent annual audit. See appendix B for more information about FISMA and other federal criteria and standards discussed in this report.

[17] The OIG provided VA with a presentation related to this inspection containing "VA Sensitive Data," as defined in 38 U.S.C. § 5727. Federal law, including FISMA and its implementing regulations, requires federal agencies to protect sensitive data and information systems due to the risk of harm that could result from improper disclosure. Accordingly, the memorandum is not being published by the OIG or distributed outside of VA to prevent intentional or inadvertent disclosure of specific vulnerabilities or other information that could be exploited to interfere with VA's network operations and adversely affect the agency's ability to accomplish its mission.

Table 1. Security Controls Evaluated by the OIG

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

Source: VA OIG analysis.

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

Security Controls

Both the Office of Management and Budget and the National Institute of Standards and Technology (NIST) provide criteria to evaluate security controls. These criteria provide requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system.[18]

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

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

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

Office of Information and Technology Structure and Responsibilities

The assistant secretary for information and technology and chief information officer leads the Office of Information and Technology (OIT). According to VA, OIT delivers available, adaptable, secure, and cost-effective technology services to VA and acts as a steward for VA's IT assets and resources. The Cybersecurity Operations Center is part of OIT's Office of Information Security. It is responsible for protecting VA information and information systems by identifying and reporting emerging and imminent threats and vulnerabilities. OIT's Office of Development, Security, and Operations unifies software development, software operations, service management, information assurance, cybersecurity compliance, performance monitoring, and technical integration throughout the entire solution delivery process. Figure 1 shows the OIT organizational structure.

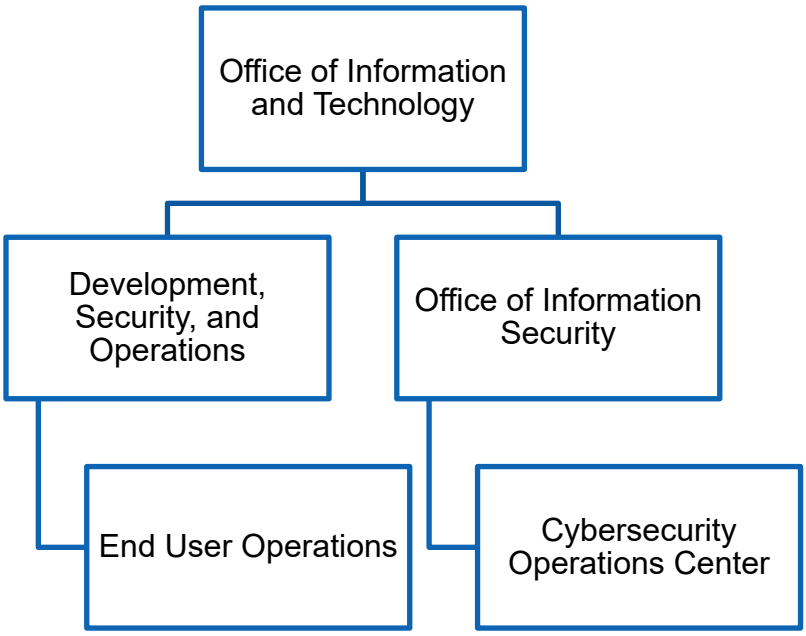

Figure 1. *Organizational structure of Office of Information and Technology entities relevant to this inspection.*
Source: VA OIG analysis.

End User Operations provides onsite and remote support to IT customers across all VA administrations and special program offices, including direct support of over 340,000 VA

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

employees and thousands of contractors who are issued government-furnished IT equipment and access. End User Operations provisions computing devices; conducts new facility activations; performs moves, adds, and changes; executes local system implementations; and engages VA's customers across the nation to meet IT support needs. OIT assigns dedicated End User Operations personnel to the Alexandria VAMC.

Results of Previous Projects

As previously mentioned, the OIG issues annual reports on VA's information security program. The FISMA audit is conducted in accordance with guidelines issued by the Office of Management and Budget and applicable NIST information security guidelines.[20] The fiscal year 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.[21] CliftonLarsonAllen LLP made 26 recommendations, listed in appendix A. Of these recommendations, all 26 are repeated from the prior annual audit, indicating that VA continues to face significant challenges in complying with FISMA requirements.[22] Repeat recommendations included addressing deficiencies in configuration management, contingency planning, security management, and access controls.

A 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.[23] According to GAO, as VA secured and modernized its information systems, VA faced several security challenges, including

- effectively implementing information security controls,
- mitigating known vulnerabilities,
- establishing elements of its cybersecurity risk management program,
- identifying critical cybersecurity staffing needs, and

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

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

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

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

- 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 unauthorized modification, disclosure and the systems will remain at risk of disruption."[24]

Alexandria VAMC

The Alexandria VAMC is in Pineville, Louisiana, and is part of the VA Alexandria Healthcare System. The VAMC supports a veteran population of more than 100,000 veterans with an active patient roster of more than 37,000. The medical center is a teaching hospital and maintains affiliations with more than a dozen universities, including Louisiana State University, Grambling State University, and Tulane University. Figure 2 is a photo of the facility.

Figure 2. *Alexandria VAMC.*
Source: VA OIG inspection team, January 13, 2022.

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

Results and Recommendations

The OIG reviewed configuration management, contingency planning, security management, and access controls at the Alexandria VAMC and only one of these four areas—contingency planning—had no deficiencies. The review showed that VA's contingency plan addressed control criteria, such as identifying essential mission and business functions; provided recovery objectives; and addressed roles and responsibilities. The team verified that the Alexandria VAMC had no critical information systems that would require an alternate processing facility.

In configuration management, the team identified deficiencies with component inventory, vulnerability management, flaw remediation, and unsupported infrastructure components. The evaluation of security management revealed a deficiency in control assessment for the VAMC's surveillance system. The team's review of access controls, including boundary protection, sensitive system resources, and physical security, identified deficiencies with improperly installed equipment, emergency power, identification and authentication, and physical security controls.

I. Configuration Management Controls

According to GAO's *Federal Information System Controls Audit Manual* (FISCAM), configuration management involves identifying and managing security features for all hardware, software, and firmware components of an information system at a given point and systematically controlling changes to that configuration during the system's life cycle. The inspection team reviewed and evaluated the 14 configuration management controls drawn from NIST criteria for VA-hosted systems at the Alexandria VAMC to determine if they met federal guidance and VA requirements.

An effective configuration management process should be described in a configuration management plan and implemented according to the plan. VA should first establish an accurate component inventory to identify all devices on the network.[25] The component inventory affects the success of other controls, such as vulnerability and patch management. OIT's Cybersecurity Operations Center identifies and reports threats and vulnerabilities for VA. Once this process is complete, OIT's Patch and Vulnerability Team develops procedures to remediate the identified issues, which can include applying patches. This process helps secure devices from attack.

Finding 1: The Alexandria VAMC Had Deficiencies in Four Configuration Management Controls

To assess configuration management controls, the inspection team interviewed the information systems owner, information system security officer, and system stewards. The team reviewed

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

local policies, procedures, and inventory lists and scanned the Alexandria VAMC's network to identify devices. The team compared the devices found on the network with the device inventories provided by VA, received vulnerability lists provided by OIT, and scanned the Alexandria VAMC's network to identify vulnerabilities.[26] Both the comparisons of the devices and the vulnerability scans showed that OIT did not have an accurate component inventory list; identify all critical or high-risk vulnerabilities in the network; or remediate flaws, including unsupported versions of applications, missing patches, and vulnerable plug-ins. Additionally, the inspection team identified unsupported infrastructure components at the VAMC.

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

Component Inventory

Previous FISMA reports have repeatedly identified inventory deficiencies as a nationwide issue for VA. Component inventories are descriptive records of IT assets in an organization down to the system level. A complete, accurate, and up-to-date inventory is required to implement an effective information security program because it provides greater awareness of and control over these systems.[27] The inspection team identified inaccuracies in the component inventory at the Alexandria VAMC, despite OIT and VA's use of an automated inventory system to maintain inventories of its information systems. VA identified 4,110 devices in the VAMC's inventory. The team identified 3,874 devices. While VA identified more devices, they did not account for all network segments and included network segments that were not reported to the team for scanning.[28] The OIG identified eight network segments with 185 devices that were not accounted for by VA. Further, there were 33 network segments with significant differences, resulting in the OIG identifying 687 more devices than were identified by VA. In total, the OIG identified 872 devices that were not accounted for by VA.

Vulnerability Management

Prior FISMA audits repeatedly found deficiencies in VA's vulnerability management. Consistent with those findings, the team identified weaknesses in vulnerability management at the Alexandria VAMC.[29] Vulnerability management is the process by which OIT identifies, classifies, and reduces weaknesses and is part of assessing and validating risks as well as monitoring the effectiveness of a security program. The Cybersecurity Operations Center

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

[27] GAO, *FISCAM*.

[28] Network segmentation is when a network is split into subnetworks. Network segmentation minimizes harm of malware and other threats by isolating it to a limited part of the network.

[29] 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."

identifies and reports threats and vulnerabilities for VA, and OIT conducts scans for vulnerabilities both routinely and randomly, or when new vulnerabilities are identified and reported. The discovered vulnerabilities are entered into a plan of action and milestones for remediation by the system steward. The system steward uses the Remediation Effort Entry Form to document mitigation or remediation efforts for each deficiency identified from the scan and provides evidence that the deficiencies have been mitigated.[30] VA requires that critical vulnerabilities be remediated within 30 days and high-risk vulnerabilities be remediated in 60 days.

NIST assigns severity levels to vulnerabilities by using the Common Vulnerability Scoring System, a framework for communicating the characteristics of software vulnerabilities.[31] The scoring system captures the principal characteristics of a vulnerability and produces a numerical score reflecting its severity. Numerical scores are classified as risk levels (low, medium, high, or critical) to help organizations properly assess and prioritize vulnerability management processes. For example, on a scale of zero to 10, critical vulnerabilities have a score between 9.0 and 10, while high-risk vulnerabilities have a score between 7.0 and 8.9.

The inspection team compared OIT-provided network vulnerability scan results from the Alexandria VAMC against its own scans conducted from January 10 to January 14, 2022. The team and OIT used the same vulnerability-scanning tools. OIT conducts scans remotely on the network segments that are identified by the system owners. However, the OIG conducts scans on site and reviews router configurations to identify all network segments. The difference in scanning location and the process for identifying network segments leads the OIG to broader results than those of OIT. The team identified 33 vulnerabilities (17 critical vulnerabilities on 8 percent of the devices and 16 high-risk vulnerabilities on 29 percent of the devices) that were not mitigated within the time frames established by OIT. Moreover, OIT's security scans did not identify five critical vulnerabilities and three high-risk vulnerabilities detected by the team. Similarly, the prior FISMA audit found that the "VA did not have a complete inventory of all vulnerabilities present on locally hosted systems."[32] While the agency is aware of many of the

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

[31] "Vulnerability Metrics," NIST National Vulnerability Database, accessed August 21, 2020, https://nvd.nist.gov/vuln-metrics/cvss; "Common Vulnerability Scoring System ver. 3.14, Specification Document, Revision 1," Forum of Incident Response and Security Teams (FIRST), accessed March 15, 2022, https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf.

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

vulnerabilities, the plan of action and milestones did not always list a remediation.[33] Further, a very small percentage of the hosts with critical vulnerabilities were accounted for in the plans of action and milestones. The OIG identified critical and high-risk vulnerabilities on 37 percent of the devices at the Alexandria VAMC. Without an effective patch management program, vulnerabilities such as security and functionality problems in software and firmware might not be mitigated, increasing opportunities for exploitation.

The medical center did not remediate all flaws affecting devices in its network. For example, the inspection team identified vulnerabilities, such as operating systems that were no longer supported by the vendor and applications with missing security patches. The flaw remediation process identifies, reports, and corrects system flaws that include installing security-relevant software and firmware updates such as patches, service packs, and malicious code signatures. Security patches are usually the most effective way to mitigate software flaw vulnerabilities. According to GAO, a patch is a piece of software code inserted into a program to temporarily fix a defect until an updated software version is released. NIST further explains that patches correct security and functionality problems in software and firmware. Patch management is how OIT acquires, tests, applies, and monitors updates that address security and functionality problems. Although patch management is a critical process used to help alleviate many of the challenges in securing systems from cyberattack, previous FISMA audits have repeatedly found deficiencies in this area.[34]

Unsupported Infrastructure Components

The inspection team noted that almost 12 percent of the Alexandria VAMC network switches used operating systems that were no longer supported by the vendor. Consequently, these devices will not receive maintenance or vulnerability support. Unsupported system components can result in an opportunity for adversaries to exploit weaknesses in the components.[35] Additionally, noncurrent software may be vulnerable to malicious code.[36] Network devices and

[33] Plans of action and milestones identify tasks needing to be accomplished. They detail resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. They also describe the measures planned to correct deficiencies identified in the controls and to address known vulnerabilities or security and privacy risks. For the purpose of inspections, the OIG considers an ongoing vulnerability mitigated if the plan of action and milestones accurately identifies the devices impacted, details mitigation efforts, and includes an accurate and timely schedule of milestones.

[34] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2021*, Report No. 21-01309-74, April 13, 2022. VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2020*, Report No. 20-01927-104, March 31, 2020. VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2019*, Report No. 19-06935-96, March 31, 2020. VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2018*, Report No. 18-02127-64, March 12, 2019.

[35] NIST Special Publication 800-53.

[36] GAO, *FISCAM*.

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

Finding 1 Conclusion

The Alexandria VAMC did not have accurate inventories, a problem that led to undetected and unaddressed critical and high-risk vulnerabilities. Consequently, vulnerability management controls did not effectively identify network weaknesses, such as unsupported versions of applications, and flaw remediation controls did not ensure comprehensive patch management. The Alexandria VAMC network devices were using old operating systems that were no longer supported and potentially vulnerable to exploitation. 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 VA missions.

Recommendations 1–3

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

1. Implement a more effective process to maintain consistent inventory information for all network segments.
2. Improve the vulnerability and flaw remediation program to accurately identify vulnerabilities and enforce flaw remediation.
3. Implement effective configuration control processes that ensure network devices maintain vendor support.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 1, 2, and 3. To address recommendation 1, the assistant secretary reported OIT has implemented physical and logical inventory changes that resulted in the VAMC complying with inventory requirements. To address recommendation 2, the assistant secretary also reported that the Cyber Security Operations Center was able to compare its scan results with the OIG's results and identify areas not typically scanned to limit the impact on patient care. Further, OIT continuously remediates and manages all its vulnerabilities through mitigation efforts and plans of action and milestones. To address recommendation 3, the assistant secretary reported that VA is developing a plan of action and milestones to address end-of-life network equipment. The full text of the response from the assistant secretary is included in appendix D.

OIG Response

OIT provided sufficient evidence to support that the corrective actions for recommendations 1 and 2 were completed. As a result, the OIG considers recommendations 1 and 2 closed. For recommendation 3, the planned corrective actions address the symptom of replacing unsupported devices. However, implementing an effective configuration control process would proactively identify and replace devices prior to their end of vendor support. The OIG will monitor implementation of the planned actions and will close the recommendation when VA provides evidence demonstrating progress in addressing the issues identified.

II. Contingency Planning Controls

Contingency planning controls are important because if they are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. To determine whether recovery plans will work as intended, they should be tested periodically in disaster-simulation exercises. FISMA requires that each federal agency implement an information security program that includes "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."[37] Although often referred to as disaster recovery or contingency plans, controls to ensure service continuity should address the entire range of potential disruptions. These may include minor interruptions, 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 Alexandria VAMC met federal guidance and VA requirements, the inspection team evaluated six contingency planning controls.

Finding 2: No Deficiencies Were Found in Contingency Planning Controls

To assess contingency planning controls, the inspection team interviewed the area manager, information system security officer, and the VAMC chief of safety and emergency management. The team also reviewed local policies and procedures.

The inspection team found that the facility's contingency plan addressed control criteria, such as identifying essential mission and business functions; provided recovery objectives; and addressed roles and responsibilities. The team verified that the Alexandria VAMC had no critical information systems that would require an alternate processing facility. Instead, the enterprise manages the systems at regional data centers. The team did not identify deficiencies in the Alexandria VAMC's contingency planning controls. Accordingly, the OIG did not make any recommendations for improvement.

[37] FISMA.

III. Security Management Controls

According to FISCAM, security management controls establish a framework and continuous cycle for assessing risk, developing security procedures, and monitoring the effectiveness of the procedures. The inspection team evaluated two security management critical elements: instituting a security management program and assessing and validating risk.[38] The team reviewed local security management policies, standard operating procedures, and applicable VA policies. These included documentation from the Enterprise Mission Assurance Support Service, VA's cybersecurity management service for workflow automation and continuous monitoring. Among the topics reviewed were assessing and validating risks, security control policies and procedures, security program effectiveness, and plans of action and milestones for known deficiencies. The team also interviewed the information system security officer, a local supervisory IT specialist, contracting officer's representative, privacy officer, and area manager. The team also conducted a walk-through of the facility.

Finding 3: The Alexandria VAMC Had a Security Management Weakness, Resulting in Multiple Deficiencies

The team's walk-through of the facility revealed a video security system that did not have an authorization to operate and consequently a lack of control assessment, which led to multiple deficiencies in the system.

Control Assessment

The video surveillance system at Alexandria VAMC did not have an authorization to operate. The team observed the system operating as intended. However, the system lacked an assessment of security controls as required by policy.[39] Previous FISMA reports have repeatedly identified security control assessment deficiencies as a nationwide issue for VA. Control assessments help to ensure organizations meet information security and privacy requirements, identify weaknesses, and deficiencies in the system design and development process and comply with vulnerability mitigation procedures.[40] Within VA, systems require an authorization to operate if they are connected to the enterprise network or have an external connection. With the lack of documentation and access, the team was unable to confirm if the system was connected to the enterprise network. However, the system did have an external connection and thus required an authorization to operate. The system was managed by local facility maintenance personnel who are not part of OIT. Due to the lack of a control assessment, the system had numerous other

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

[39] Control assessments involves testing or evaluation of the controls in an information system or an organization to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security or privacy requirements for the system or the organization.

[40] NIST Special Publication 800-53.

deficiencies, such as unsupported network infrastructure equipment, a vulnerable network operating system, and improperly protected credentials. Further, the team that maintained the equipment did not have access to configuration information used to manage the system and therefore relied on an external contractor to maintain the system. Without measures in place to assess controls, vulnerabilities existed that could adversely impact the integrity and protection of the video surveillance system.

Recommendation 4

The OIG made the following recommendation to the Alexandria VA Medical Center director:

4. Perform security control assessments of the video surveillance system and obtain an authorization to operate in accordance with set policy.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendation 4. The assistant secretary reported OIT is incorporating the video surveillance system into the Alexandria special-purpose system for assessment and authorization. The full text of the response from the assistant secretary is included in appendix D.

OIG Response

The assistant secretary's planned corrective actions for recommendation 4 are responsive to the intent of the recommendation. The OIG will monitor implementation of the planned actions and will close the recommendation when VA provides evidence demonstrating progress in addressing the issues identified.

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. Identification, authentication, and authorization controls ensure that users have the proper access and are restricted to authorized individuals. Accordingly, the inspection team reviewed these three critical access control elements.[41]

Finding 4: The Alexandria VAMC Had Deficiencies in Access Controls

To evaluate the Alexandria VAMC's access controls, the inspection team interviewed the information system security officer, area manager, a local supervisory IT specialist, and the police chief; reviewed local policies and procedures; conducted walk-throughs of the facility; and analyzed audit logs.[42]

The OIG found issues with access controls at the Alexandria VAMC, including

- improperly installed network infrastructure equipment,
- failed uninterruptible power supplies supporting network infrastructure equipment,
- identity and authentication management controls that did not meet organizational requirements, and
- an outdated physical access control system.

Improper Equipment Installation

The Alexandria VAMC did not properly install network infrastructure equipment. While VA establishes standards for network equipment installation, those standards were not followed for some network equipment. For example, the team identified three instances of network equipment not mounted to equipment racks. Consequently, the unsecured devices are susceptible to damage, which can interrupt the availability of information to portions of the network serviced by that device. Further, some of the equipment is stacked on top of each other, which does not allow for proper cooling and can cause equipment failure due to overheating.

Emergency Power

During a walk-through, the OIG inspection team found an uninterruptible power supply supporting the VAMC that was not operational and a second power supply with a failed battery. An uninterruptible power supply is an electrical system or mechanism that provides emergency

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

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

power when there is a failure of the main power source.[43] They are typically used to protect devices, datacenters, and telecommunications equipment where an unexpected disruption could cause injuries, fatalities, serious mission or business disruption, or loss of data or information. Uninterruptible power supplies differ from emergency power systems for backup generators because they provide near-instantaneous protection from interruptions. OIT personnel responsible for maintenance of the network equipment were not conducting routine maintenance that should have detected and replaced the failed uninterruptible power supply and battery. Without operational uninterruptible power supplies, the infrastructure equipment will not function during power fluctuations or outages, resulting in interruption of data flow and disruption of access to network resources.

Identification and Authentication

The OIG identified databases that do not enforce password changes in accordance with VA information security policy. The inspection team's scan results also discovered that the database servers allow local credentials that rely on weak, single-factor authentication to provide system access. Identification and authentication controls distinguish one user from another and establish the validity of a user's claimed identity.[44] The effects of weak password policies could result in the loss of protected health information or disruption of VAMC operations. Furthermore, the OIG noted that VA passwords were not set to expire on servers in accordance with VA policy. According to OIT, the weak password settings are required for older applications to prevent them from "breaking." However, OIT also acknowledged that deviations from the policy were not approved. Weak password controls expose organizations to a greater risk of compromise. Once compromised, a local database account could be used for unauthorized disclosure or modification of personal health information.

Physical Access

The standalone physical access controls system used for the data center and core switch room was using an outdated operating system and did not produce audit logs, which is contrary to VA policy. In accordance with VA policy, the site is required to monitor physical access where information systems reside and review access logs quarterly. Due to a lack of logging capability, it would be difficult to identify potential security incidents and suspicious activities, such as access outside of normal work hours, unusual length of time, or out-of-sequence access. Further, the standalone system is using an outdated operating system that is no longer supported by the vendor. As a result, the system is a higher security risk and more susceptible to computer viruses. The outdated system would also be difficult to replace, thereby creating a potential single point of failure to the datacenter and core switch room. The facility does have a centralized,

[43] NIST Special Publication 800-53.

[44] GAO, *FISCAM.*

campus-wide physical access control system; however, it is not currently being used for the datacenter and core switch room.

Finding 4 Conclusion

The Alexandria VAMC did not have properly installed equipment, which could interrupt the availability of information to portions of the network. Additionally, there was a nonoperational uninterruptible power supply and one with a failed battery that would not protect equipment in case of a power outage. Databases were using weak authentication and password controls. Finally, the VAMC was using a physical access control system that did not meet logging requirements and was using an outdated operating system. Unless the VAMC takes corrective actions, it risks unauthorized access to critical network resources, inability to respond effectively to incidents, or loss of personally identifiable information.

Recommendations 5–8

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

5. Ensure installation of distributed network infrastructure equipment that meets VA installation standards, to include proper equipment mounting and clearance.
6. Ensure routine maintenance is conducted on uninterruptible power supplies.
7. Implement database authentication processes that comply with VA security requirements.

The OIG made the following recommendation to the Alexandria VA Medical Center director:

8. Implement a physical access control system for the data center and core switch room that is supportable and can meet VA logging requirements.

Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 5, 6, 7, and 8. To address recommendations 5 and 6, the assistant secretary reported that OIT has submitted purchase orders for installation of switch racks and that VA conducted maintenance and replaced batteries in the uninterruptible power supplies. In response to recommendation 7, the assistant secretary reported that OIT's database management service line published policy and procedures for compliance with database authentication and deployment of baselines. Finally, to address recommendation 8, the assistant secretary reported that a contract has been awarded to install a physical access control system for the data center and core switch room that is supportable and meets VA logging requirements. The full text of the response from the assistant secretary is included in appendix D.

OIG Response

OIT provided sufficient evidence to support that the corrective actions regarding recommendations 6 and 7 were completed. As a result, the OIG considers recommendations 6 and 7 closed. For recommendation 5, switch racks allow secure installation of equipment to prevent damage, tampering, or theft and are vented to promote airflow to keep equipment cool. For recommendations 5 and 8, the planned corrective actions 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 evidence demonstrating progress in addressing the issues identified.

Overall Conclusion

The inspection team identified deficiencies in component inventory, vulnerability management, flaw remediation, baseline configurations, security management, improper equipment installation, emergency power, identification and authentication, and physical security controls. The OIG made six recommendations to the assistant secretary for information and technology and chief information officer: implement a more effective process to maintain consistent inventory information for all network segments; improve the vulnerability and flaw remediation program to accurately identify vulnerabilities and enforce flaw remediation; establish effective configuration control processes that ensure network devices maintain vendor support; ensure proper installation of network equipment; conduct routine maintenance on uninterruptible power supplies; and implement database authentication processes that comply with VA security requirements. The OIG also made two recommendations to the Alexandria VAMC director, including performing security control assessments for the video surveillance system seeking an authorization to operate and implementing a physical access control security system that is supportable and can meet VA security standards. Although the information and recommendations in this report are based on findings specific to the Alexandria VAMC, other facilities across VA could benefit from reviewing this information and considering these recommendations.

Appendix A: FISMA Audit for Fiscal Year 2021 Report Recommendations

In the FISMA audit for fiscal year 2021, CliftonLarsonAllen LLP made 26 recommendations. Of these, all 26 were repeat recommendations from the prior year. The FISMA audit assesses the agencywide security management program, and recommendations in the FISMA report are not specific to the Alexandria VAMC. 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 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 our assessments of VA's web applications, database platforms, network infrastructure, and workstations.
13. Maintain a complete and accurate security baseline configuration for all platforms and ensure all baselines are appropriately monitored for compliance with established VA security standards.
14. Implement improved network access controls that restrict medical devices from systems hosted on the general network.
15. Consolidate the security responsibilities for networks not managed by the Office of Information and Technology, under a common control for each site and ensure vulnerabilities are remediated in a timely manner.
16. Implement improved processes to ensure that all devices and platforms are evaluated using credentialed vulnerability assessments.
17. Implement improved procedures to enforce standardized system development and change control processes that integrates information security throughout the life cycle of each system.
18. Review system boundaries, recovery priorities, system components, and system interdependencies and implement appropriate mechanisms to ensure that established system recovery objectives can be measured and met.
19. Ensure that contingency plans for all systems are updated to include critical inventory components and are tested in accordance with VA requirements.
20. Implement more effective 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.
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 POA&Ms.

24. Fully develop a comprehensive list of approved and unapproved software and implement continuous monitoring processes to prevent the use of prohibited software on agency devices.
25. Develop a comprehensive inventory process to identify connected hardware, software, and firmware used to support VA programs and operations.
26. Implement improved procedures for monitoring contractor-managed systems and services and ensure information security controls adequately protect VA sensitive systems and data.

Appendix B: Background

Federal Information System Controls Audit Manual

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

FISCAM breaks configuration management controls into the following critical elements.

- **Develop and document configuration management policies, plans, and procedures** at the entity, system, and application levels to ensure effective configuration management processes. These procedures should cover employee roles and responsibilities, change control, system documentation requirements, establishment of decision-making structure, and configuration management training.
- **Maintain current configuration information,** which involves naming and describing physical and functional characteristics of a controlled item, as well as performing activities to define, track, store, manage, and retrieve configuration items. Examples of these controls are baseline configurations, configuration settings, and component inventories.
- **Authorize, test, approve, and track changes** by formally establishing a change management process, with management's authorization and approval of the changes. This element includes documenting and approving test plans, comprehensive and appropriate testing of changes, and creating an audit trail to clearly document and track changes.
- **Conduct routine configuration monitoring** to determine the accuracy of the changes that should address baseline and operational configuration of hardware, software, and firmware.[45] 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

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

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

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

FISCAM identifies the following critical elements for contingency planning:

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

FISCAM has seven critical elements for security management:

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

- **Document and implement security control policies and procedures** that appropriately address general and application controls and ensure users can be held accountable for their actions. These controls, which are more general at the entity-wide level and more specific at the system level, should be approved by management.
- **Implement security awareness and personnel policies** that provide training for new employees, contractors, and users; periodic refresher training; and distribution of security policies detailing rules and expected behaviors. This element also addresses hiring, transfers, terminations, and performance for employees, contractors, and users. Examples of controls in this area are security awareness training, rules of behavior, position categorization, personnel policies, personnel screening, termination, transfer, access agreements, third-party personnel security, and personnel sanctions.
- **Monitor the program** to ensure that policies and controls effectively reduce risk on an ongoing basis. Effective monitoring involves testing controls to evaluate and determine whether they are appropriately designed and operating effectively. Examples of these controls are security assessments, continuous monitoring, privacy impact assessments, and vulnerability scanning.
- **Remediate information security weaknesses** when they are identified, which involves reassessment of related risks, applying appropriate corrective actions, and follow-up monitoring to ensure actions are effective. Agencies develop plans of actions and milestones to track weaknesses and corresponding corrective actions.
- **Ensure third parties are secure,** as vendors, business partners, and contractors are often granted access to systems for purposes such as outsourced software development or system transactions.[46]

FISCAM lists six access control critical elements:

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

[46] GAO, *FISCAM*.

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

Federal Information Security Modernization Act of 2014

The stated goals of FISMA 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

[47] FISMA.

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

NIST Information Security Guidelines

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

Appendix C: Scope and Methodology

Scope

The inspection team conducted its work from December 2021 through June 2022. The team evaluated configuration management, contingency planning, security management, and access controls of operational VA IT assets and resources in accordance with FISMA, NIST security guidelines, and VA's IT security policy. In addition, the team assessed the capabilities and effectiveness of IT security controls used to protect VA systems and data from unauthorized access, use, modification, or destruction.

Methodology

To accomplish the objective, the inspection team examined relevant laws and policies; inspected the facility and systems for security compliance; and interviewed VA personnel responsible for the Alexandria VAMC's IT security and operations, privacy compliance, and human resources management. The team conducted vulnerability and configuration testing to determine local systems' security compliance. Finally, the team analyzed the results of testing, interviews, and the inspection to identify policy violations and threats to security.

Internal Controls

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

The team used GAO's FISCAM as a template to plan for inspections. When planning for this review, the team identified potential information system controls that would significantly impact the review. Specifically, the team used FISCAM appendix II as a guide to help develop evidence requests and a base set of interview questions for the Alexandria VAMC and its personnel. The team used the FISCAM controls identified in appendix B as an overlay to correlate FISMA controls used by VA to protect and secure their information systems. Although similar to the contractor-conducted annual FISMA audits, this review focused on security controls that are implemented at the local level. However, there are some controls that overlap and are examined 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 Alexandria VAMC aligned with the control activities category. Control activities are the actions management establishes

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

Fraud Assessment

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

Data Reliability

The inspection team generated computer-processed data by using network-scanning tools. The results of the scans were provided to the OIT Quality and Compliance Readiness Office. The team used industry standard information system security tools to identify information systems on the VA network and to take snapshots of their configurations, which were used to identify vulnerabilities. In this process, the team was not testing VA data or systems for transactional accuracy. The security tools identified a version of software present on a system and then compared it to the expected version. If the system did not have the current software version, the tool identified that as a vulnerability. As the security tools did not alter data, the team determined that the output was reliable. The data were complete and accurate, met intended purposes, and were not subject to alteration.

Government Standards

The OIG conducted this review in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.

Appendix D: VA Management Comments

Department of Veterans Affairs Memorandum

Date: July 26, 2022

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

Subj: OIG Draft Report: Inspection of Information Technology Security at the Alexandria VA Medical Center in Louisiana, Project Number 2022-00971-AE-0046 (VIEWS 07948144)

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

1. The Office of Information and Technology (OIT) is responding to the Office of Inspector General (OIG) draft report, *Inspection of Information Technology Security at the Alexandria VA Medical Center in Louisiana* (Project Number 2022-00971-AE-0046).
2. OIT submits written comments, supporting documentation and a target completion date for each recommendation.

The OIG removed point of contact information prior to publication.

(Original signed by)

Kurt D. DelBene

Attachment

Attachment

Office of Information and Technology Comments on Office of Inspector General Draft Report,

Inspection of Information Technology Security at the Alexandria VA Medical Center in Louisiana, Project Number 2022-00971-AE-0046

(VIEWS 07948144)

Recommendation 1: Implement more effective inventory management tools for all network segments.

Comments: Concur.

The Department of Veterans Affairs (VA) Office of Information and Technology (OIT) has implemented the following changes since receipt of audit findings related to *accountability (physical)* management:

Inventory compliance (items updated within the last 365 days) was 98% as of June 18, 2022. The expected compliance level is 95%.

Corporate Data Warehouse is the system of record for system component inventory of physical hardware assets.

Changes since receipt of audit findings related to *visibility (logical)* management include: Enterprise-wide:

- The Enterprise Mission Assurance Support Service (eMASS) is the system inventory of accredited information systems/Authority to Operate boundaries.
- VA established an enterprise integrated product team to review and analyze scanning deltas to resolve gaps in logical inventory reporting as part of ongoing operational activities.
- OIT Enterprise Federal Information Security Modernization Act (FISMA) Containerization Asset to Boundary (FCAB) project implementation electronically aligns assets to their new FISMA system boundaries in eMASS. FCAB project implementation reduces the human factor of manually generating and uploading the asset list to eMASS, allowing easier identification of system owners of device assets, better vulnerability management and future baseline configuration capabilities. Expected VA-wide FCAB project completion date is November 30, 2022.

Facility-specific:

- VA updated the Alexandria VA Medical Center accreditation boundary to include infrastructure and storage devices, to facilitate scanning and vulnerability remediation based on internet protocol range and help prevent duplicate accounting of assets in electronic eMASS inventory.

VA requests closure of recommendation 1.

VA provided supporting evidence in Appendix A, Recommendation 1.

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

Comments: Concur.

VA OIT concurs with the OIG's findings and recommendation related to vulnerability management and flaw remediation. Within the timeframe of the overall inspection, VA OIT was able to demonstrate vulnerability identification, remediation, mitigation and management rates at the Alexandria VA Medical Center of 99.75% for all critical and high vulnerabilities. OIT ingested the OIG scan data into the OIT vulnerability management tracking tool and the comparison demonstrated that OIT had the same

vulnerabilities with a 0% variance – some initial data variance may be detected due to the time difference between VA scans, OIG scans and Provided-by-Client scan deliverables.

VA OIT continuously remediates and manages all its vulnerabilities through mitigation efforts and Plans of Action and Milestones (POA&M). OIT is implementing the next level of maturity with the establishment of enterprise risk tolerance for vulnerability management.

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

Cyber Security Operations Center (CSOC) performed a crosswalk comparison of OIG scans against VA scans to identify differences. OIG had findings in the Common Gateway Interface abuses cross site scripting, or XXS, family that VA had not found because that family is disabled per VA policy. This is a common action to prevent negatively effecting systems that may impact patient care.

CSOC also noted a key subnet mentioned by OIG is a Veterans Health Information Systems and Technology Architecture (VistA) imaging range which VA scans separately. VA maintains the VistA imaging data in a separate scan bucket and can provide if needed. Analysis has shown that these subnets and subsequent/related findings are likely behind protected virtual local area networks (VLAN) for which VA does not maintain standard scan visibility to minimize business or patient care impact, while the OIG scans maintain visibility to those protected VLANs.

VA requests closure of recommendation 2.

VA provided supporting evidence in Appendix A, Recommendation 2.

Recommendation 3: System owners should implement more effective configuration control processes to ensure network devices are maintained in accordance with OIT security standards.

Comments: Concur.

VA OIT concurs with the OIG recommendation to implement a more effective configuration control process. VA is developing a POA&M to address the end-of-life network equipment.

Expected Completion Date: November 30, 2022.

Recommendation 4: Perform security control assessments of the video surveillance system and obtain an authorization to operate in accordance with set policy.

Comments: Concur.

- Area Alexandria – special purpose systems information system owner (ISO) (Area Manager) shall ensure the local system (site) control provider (SPS) and business owner adhere to published guidance to submit a security service request within ServiceNow (SNOW) to initiate the completion of an enterprise risk analysis (ERA) (security control analysis) for all SPS requiring a VA network connection.
    - The ERA process enables VA to assess and manage cybersecurity risks, identify mitigating controls and catalog device/system-specific risk assessments for specialized device /systems (SD/S) enterprise-wide. Additionally, the ERA process comprehensively addresses the unique requirements of network-connected SD/S and implementation of mitigation controls to reduce the overall VA security risk. Guidance is in accordance with VA Directive 6500, VA Cybersecurity Program; VA Handbook 6500, Risk Management

Framework for VA Information Systems - Tier 3: VA Information Security Program, and National Institute of Standards and Technology Special Publication 800-37 Revision 2 Risk Management Framework Information Systems and Organizations.

- Area Alexandria – special purpose system ISO shall identify the local SPS and/or business owner who shall submit the security service request via SNOW intake process.
- Specialized Device Cybersecurity Department shall conduct the ERA on the video surveillance system once the security service request is submitted. The ERA will be completed within the established/published service level agreement of 43 working days.
- Area Alexandria – special purpose system ISO shall ensure the system/device is incorporated into the appropriate information system assessment and authorization boundary in accordance with VA's Risk Management Framework.

Expected Completion Date: December 31, 2022.

VA provided supporting evidence in Appendix A, Recommendation 4.

Recommendation 5: Ensure installation of distributed network infrastructure equipment that meets VA 567 installation standards, to include proper equipment mounting and clearance.

Comments: Concur.

Buildings on the Alexandria campus are more than 100 years old, and closets are non- standard in size and location. Local OIT will submit purchase orders for the local engineering service to install switch racks in closets that do not currently have racks.

Expected Completion Date: June 30, 2023.

Recommendation 6: Ensure routine maintenance is conducted on uninterruptible power supplies.

Comments: Concur.

VA conducted routine maintenance on uninterruptible power supplies and submitted a Maximo ticket for facility electricians to replace batteries.

Completed April 21, 2022. VA requests closure of recommendation 6. VA provided supporting evidence in Appendix A, Recommendation 6.

Recommendation 7: Implement database authentication processes that comply with VA security requirements.

Comments: Concur.

VA OIT Database Management Service Line (DMSL) concurs with the finding that some database authentication processes were not approved, as there was no written policy outlining appropriate settings. To correct the finding that deviations were not approved, DMSL published policy and procedures outlining compliance with VA security requirements regarding database authentication processes. The DMSL Service Line Manager signed the Internal Operating Procedure on Structured Query Language baseline deployment.

Completed April 18, 2022. VA requests closure of recommendation 7. VA provided supporting evidence in Appendix A, Recommendation 7.

Recommendation 8: Implement a physical access control system for the data center and core switch room that is supportable and can meet VA logging requirements.

Comments: Concur.

VA awarded a contract to Deep South Systems Integration to install a physical access control system for the data center and core switch room that is supportable and can meet VA logging requirements.

Expected Completion Date: November 30, 2022.

VA provided supporting evidence in Appendix A, Recommendation 8.

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/Audit/Review Team	Michael Bowman, Director Ginalynn Alvarado Jack Henserling Kimberly Moss Adam Sowells Brandon Zahn
Other Contributors	Charles Hoskinson Clifford Stoddard

Report Distribution

VA Distribution

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

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget
U.S. Senate: Bill Cassidy and John Kennedy
U.S. House of Representatives: Troy Carter, Garret Graves, Clay Higgins, Mike Johnson, Julia Letlow, and Steve Scalise

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