US DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS HEALTH ADMINISTRATION

Inspection of Information Security at the Northern Arizona VA Healthcare System

Information Security Inspection	22-04104-112	July 11, 2023

BE A
VOICE FOR VETERANS
REPORT WRONGDOING
va.gov/oig/hotline | 800.488.8244

OUR MISSION

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

CONNECT WITH US

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

PRIVACY NOTICE

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

Executive Summary

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

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

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

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

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

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

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

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

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

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

2. **Security management controls** "establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of the procedures."[6]
3. **Access controls** provide reasonable assurance that computer resources are restricted to authorized individuals. Access also includes physical and environmental controls associated with physical security, such as authorization, visitors, monitoring, delivery, and removal.[7]

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

What the Inspection Found

The OIG identified deficiencies in all three areas: configuration management, security management, and access controls.

Four Configuration Management Controls Had Deficiencies

The Northern Arizona VA Healthcare System had deficiencies in four configuration management controls:

- **Vulnerability management** is the process by which the Office of Information and Technology (OIT) identifies, classifies, and reduces weaknesses.
- **Flaw remediation** is how organizations correct software defects and often includes system updates, such as security patches.[8]
- **Unsupported components** occur when developers no longer update their products.
- **Baseline configurations** are documents, formally reviewed and agreed-upon specifications that serve as the basis for future builds, and releases or changes to systems that include security and privacy control implementation.[9]

VA has a vulnerability management program, but it can be improved. Prior FISMA audits repeatedly found deficiencies in VA's vulnerability management. Consistent with those findings, the team found operating systems that were no longer supported by the vendor and applications

[6] GAO, *FISCAM*.

[7] GAO, *FISCAM*.

[8] NIST Special Publication 800-53.

[9] OIT Enterprise Systems Engineering System Design and Core SE Services, "SQL Server 2012 Baseline Configuration," ver. 3.1, July 12, 2017.

with missing security patches at the healthcare system. OIT scans for vulnerabilities routinely, randomly, and when new vulnerabilities are identified and reported. Although the inspection team and OIT used the same vulnerability-scanning tools, the team found vulnerabilities that OIT did not detect. For example, the OIG found 83 critical vulnerabilities that OIT did not. The inspection team also identified 245 vulnerabilities—112 critical vulnerabilities on 2 percent of the devices and 133 high-risk vulnerabilities on 47 percent of the devices—that were not mitigated within the required 30- or 60-day windows. Interviews with personnel responsible for local vulnerability remediation indicated that they prioritize critical vulnerability remediation. The low percentage of critical vulnerabilities supports that claim. While OIT is aware of many of the vulnerabilities, the plans of actions and milestones did not always list remediations.[10]

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

The OIG noted that 71 out of 80 of the healthcare system's network switches used operating systems that did not meet OIT baseline requirements and 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 components.[11] Additionally, noncurrent software may be vulnerable to malicious code.[12] Network devices and IT systems are critical infrastructure to an organization.[13] Upgrading is not just a defensive strategy but a practical one that protects network stability.

The OIG identified a local database with multiple vulnerabilities caused by configurations that deviated from the OIT baseline. After the OIG made the system steward aware of this issue, he began the process of moving the application to the VA Enterprise Cloud, where baseline configurations can be applied and managed by the Database Management Service Line. Data stored in a database has become a more frequent target for malicious users. Such attacks can result in identity theft, financial loss, loss of privacy, a breach of national security, or other types of corruption that can result from unauthorized access to sensitive data. Without managing and applying baseline configuration, OIT is unaware of weaknesses that could adversely impact the database.

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

[11] NIST Special Publication 800-53.

[12] GAO, *FISCAM*.

[13] "Silent Risk—Why We Must Upgrade Network Software," Cisco, accessed December 22, 2022, https://www.cisco.com/c/dam/en_us/about/security/cspo/docs/perspective_silent_risk.pdf.

One Security Management Control Was Deficient

The OIG identified one security management control weakness: continuous monitoring of the inventory was deficient. The inspection team discovered almost twice the number of devices on the network when compared to those identified in the Enterprise Mission Assurance Support Service (eMASS), VA's cybersecurity management service for workflow automation and continuous monitoring. OIT provided an inventory that was close to the inventory the team identified, leading the team to determine that OIT is aware of the devices in use but was not routinely updating the inventory in eMASS. Continuous monitoring facilitates ongoing awareness of the system security and privacy posture to support organizational risk management decisions. A key component of VA's continuous monitoring program is frequent updates to hardware and software inventories. Continuous monitoring reports and metrics in eMASS provide management with information about the system and its security posture, which in turn supports risk management and authorization decisions. By not routinely updating the hardware inventory, management is making risk decisions based on inaccurate system information.

Seven Access Controls Had Deficiencies

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

- **Physical access** includes devices and barriers to prevent movement from publicly accessible areas to nonpublic areas.[14]
- **Video surveillance** is the use of cameras installed at strategic locations and is required for data centers.[15]
- **Environmental controls** maintain and monitor temperature and humidity where communication equipment is located.[16]
- **Equipment installation** ensures equipment is installed according to established standards, reducing risk of damage.
- **Emergency power** provides near-instantaneous protection from unanticipated power interruptions.
- **Fire protection controls** prevent potential damage to facilities or interruptions in service.

[14] NIST Special Publication 800-53.

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

[16] NIST Special Publication 800-53.

- **Water detection** senses the presence of water in the vicinity of information systems.

The OIG discovered multiple communication rooms where physical access was not effectively controlled. The healthcare system had an automated physical access control system in which staff use badges to enter buildings and rooms. However, the system was not fully deployed or operational. Instead, employees routinely use keys to gain access. Key inventories, which are required every six months, have not been conducted at the facility in more than two years due to locksmith turnover and a failure to accurately track key distribution. The facility manager stated, "People had keys that weren't logged so the logging failed, and we aren't sure who has keys right now." As a result, the facility is replacing the entire key system. On September 30, 2022, a contract was awarded for the new key system. Restricting physical access protects IT resources from loss or impairment.

The inspection team discovered that the healthcare system had no video surveillance system for the data center at its main campus, the Bob Stump VA Medical Center. The facility did have camera systems in the patient care buildings. The healthcare system is in the process of upgrading its surveillance system, which would significantly expand its surveillance capability. Ineffective monitoring of activities supporting information systems minimizes the facility's incident response capabilities in the event of a security compromise. The lack of an effective incident response can undermine management's awareness of security vulnerabilities that could hinder the operation of mission-critical systems.

During walk-throughs, the inspection team discovered several communication rooms without temperature or humidity controls. Temperature extremes can reduce efficiency and lead to other problems, including premature aging and failure of equipment. High humidity can corrode internal components and cause degradation of electrical functions. Insufficient environmental controls can have a significant adverse impact on the availability of systems needed to support the organizational mission and business functions.[17]

The healthcare system did not properly install network infrastructure equipment. The team identified five instances of network equipment not mounted to racks. Unsecured devices are susceptible to damage, which can interrupt the availability of information to portions of the network serviced by the device. Further, the team found stacked equipment, which impedes proper cooling and can cause premature equipment failure due to overheating.

The team also found several communication rooms without uninterruptible power supplies. An uninterruptible power supply is an electrical system or mechanism that provides emergency power when there is a failure of the main power source.[18] Without operational uninterruptible

[17] NIST Special Publication 800-53.

[18] NIST Special Publication 800-53.

power supplies, equipment will not function during power fluctuations or outages, resulting in interruption of data flow and disruption of access to network resources.

The team discovered 11 communication rooms missing fire-detection or suppression controls. VA requires fire suppression and detection systems—such as sprinkler systems, fire extinguishers, fixed fire hoses, and smoke detectors—to prevent potential damage to facilities or interruptions in service. During the walk-through, the team determined that the data center lacked water sensors. Facility staff were unsure whether water sensors were installed, and the inspection team was unable to identify water sensors where they should have been located. OIT requires facility management and the area manager to be alerted when automated mechanisms detect the presence of water in the vicinity of the information system. Without water sensors, VA would not be able to minimize losses or prevent incidents by detecting leaks early.

What the OIG Recommended

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

1. Implement a more effective vulnerability management program to address security deficiencies identified during the inspection.
2. Ensure vulnerabilities are remediated within established time frames.
3. Ensure the unmanaged database completes the transition to the VA Enterprise Cloud where it can be managed and have security baselines applied.
4. Implement more effective configuration control processes to ensure network devices maintain vendor support.
5. Implement an improved inventory process to ensure that all connected devices used to support VA programs and operations are documented in the Enterprise Mission Assurance Support Service.
6. Ensure network infrastructure equipment is properly installed.

The OIG also made five recommendations to the Northern Arizona VA Healthcare System director:

7. Ensure physical access controls are implemented for communication rooms.
8. Ensure a video surveillance system is operational and monitored for the data center.
9. Ensure communication rooms with infrastructure equipment have adequate environmental controls.
10. Ensure communication rooms with infrastructure equipment have fire-detection and suppression systems.

11. Ensure water detection sensors are implemented in the data center.

VA Management Comments and OIG Response

The assistant secretary for information and technology and chief information officer concurred with all 11 recommendations. Responsive actions plans were submitted for all recommendations except one. While the response to recommendation 9 did not address the recommendation, evidence was provided that allowed the OIG to validate that actions had been taken to meet the intent of the recommendation, and the OIG considers it closed. The assistant secretary provided evidence to support actions addressing recommendations 3 and 4 were completed, and the OIG also considers these recommendations closed.

The assistant secretary reported that actions addressing recommendations 5, 7, 8, and 11 were in progress. The 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. The corrective actions for recommendations 6 and 10 are responsive to the intent of the recommendations; however, the assistant secretary did not provide sufficient evidence to support closure of the recommendations.

The assistant secretary concurred with recommendation 1 and 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 own scan results that the OIG received on April 19, 2023, showed that 57 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 also stated that VA's overall patch and vulnerability compliance percentages provide evidence that VA has implemented, and is managing, an effective vulnerability program. However, this statement runs counter to the OIG's results, which showed 245 vulnerabilities (112 critical-risk vulnerabilities on 2 percent of the devices and 133 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 83 critical-risk vulnerabilities the OIG detected.

The assistant secretary also concurred with recommendation 2 and stated that VA can provide evidence of remediation of vulnerabilities that persist beyond established remediation time frames. However, no evidence was provided that would allow the OIG to validate the claim. 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. The full text of the response from the assistant secretary is included in appendix D.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

Contents

Abbreviations

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

Introduction

Information security controls protect VA systems and data from unauthorized access, use, modification, or destruction. To determine compliance with the Federal Information Security Modernization Act of 2014 (FISMA), the VA Office of Inspector General (OIG) contracts with an independent public accounting firm that conducts an annual audit of VA's information security program and practices.[19] 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.[20]

In 2020, the OIG also started an information security inspection program. These inspections assess whether VA facilities are meeting federal security requirements that protect systems and data from unauthorized access, use, modification, or destruction.[21] They are typically conducted at selected facilities that have not been assessed in the sample for the annual FISMA audit or at facilities that previously performed poorly. Inspections provide recommendations to VA on enhancing information security oversight at local and regional facilities.[22] Appendix C provides more detail on the inspection scope and methodology.

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

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

Security Controls

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

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

[20] National Institute of Standards and Technology (NIST) Special Publication 800-53, rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020, includes updates as of December 10, 2020. Appendix A details the 26 recommendations that resulted from the fiscal year 2022 FISMA audit.

[21] Formerly, the inspection looked at four control areas; however, contingency planning is largely enterprise controlled and is not a significant risk at the local level. Appendix B presents background information on federal information security requirements.

[22] 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.

monitoring, reviewing, maintaining, and improving a documented information security management system.[23]

According to VA Handbook 6500, responsibility for developing and maintaining information security policies, procedures, and control techniques lies with the assistant secretary for information and technology, who also serves as VA's chief information officer. In addition, VA Handbook 6500 describes the risk-based process for selecting system security controls, including the operational requirements.[24] VA established guidance outlining both NIST- and VA-specific requirements to help information system owners select the appropriate controls to secure their systems.

The OIG information security inspections are focused on three security control areas that apply to local facilities and have been selected based on their level of risk, as shown in table 1.[25]

Table 1. Security Controls Evaluated by the OIG

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

Source: VA OIG analysis.

Without these critical controls, VA's systems are at risk of unauthorized access or modifications. A cyberattack could destroy, disrupt access to, or allow malicious control of personal

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

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

[25] The OIG recently removed a fourth control area—contingency planning—from its information security inspections because this area is largely enterprise controlled and not a significant risk at the local level.

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 information technology (IT) assets and resources. The Cybersecurity Operations Center, which is part of OIT's Office of Information Security, is responsible for protecting VA information and information systems by identifying and reporting emerging and imminent threats and vulnerabilities. OIT's Office of Development, Security, and Operations unifies software development, software operations, service management, information assurance, cybersecurity compliance, performance monitoring, and technical integration throughout the entire solution delivery process.

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

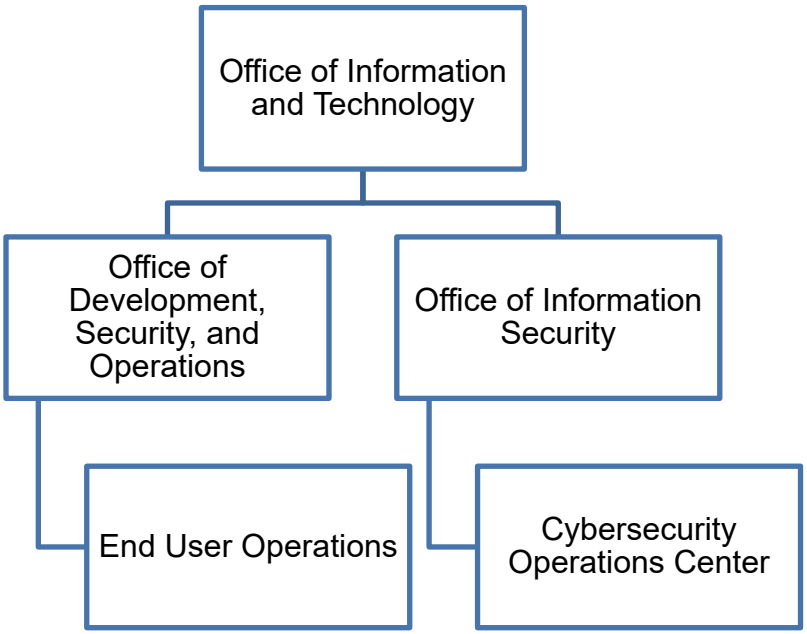

Figure 1. *Organizational structure of Office of Information and Technology entities relevant to this inspection.*

Source: VA OIG analysis.

End User Operations provides onsite and remote support to IT customers across all VA administrations and special program offices, including direct support of approximately 400,000 VA employees and over 100,000 contractors who are issued government-furnished IT

equipment and access. End User Operations provisions computing devices; conducts new facility activations; performs moves, adds, and changes; executes local system implementations; and engages VA's customers across the nation to meet IT support needs. OIT assigns dedicated End User Operations and Office of Information Security personnel to the Northern Arizona VA Healthcare System, including system stewards who are responsible for managing system plans of action and milestones to ensure all assessed and scanned vulnerabilities are documented.

Results of Previous Projects

As previously mentioned, the OIG issues annual reports on VA's information security program. The FISMA audit is conducted in accordance with guidelines issued by the Office of Management and Budget and applicable NIST information security guidelines.[26] The fiscal year 2022 FISMA audit, conducted by independent public accounting firm CliftonLarsonAllen LLP, evaluated 47 major applications and general support systems hosted at 23 VA facilities, including the testing of selected management, technical, and operational controls outlined by NIST.[27] 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.[28] Repeat recommendations included addressing deficiencies in configuration management, security management, and access controls.

A statement prepared by the Government Accountability Office (GAO) for a House Veterans' Affairs subcommittee hearing in November 2019 said VA was one of the federal agencies that continued to have a deficient information security program.[29] According to GAO, VA faced several security challenges while securing and modernizing its information systems, including

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

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

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

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

[29] Government Accountability Office (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 increased risk of unauthorized modification and disclosure, and the system will remain at risk of disruption."[30]

Northern Arizona VA Healthcare System

The Northern Arizona VA Healthcare System provides healthcare services to veterans throughout northern Arizona, spanning 65,000 square miles. The healthcare system provides primary care and specialty health services, including mental health, audiology, speech, dentistry and oral surgery, low vision and blind rehabilitation, physical therapy, recreation and creative arts therapy, and women's health service. The healthcare system's main campus is the Bob Stump VA Medical Center in Prescott, Arizona.

Figure 2. *Bob Stump VA Medical Center.*
Source: https://www.va.gov/northern-arizona-health-care/, December 1, 2022.

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

Results and Recommendations

I. Configuration Management Controls

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

An effective configuration management process should be described in a configuration management plan and implemented according to the plan.[31] VA should first establish an accurate component inventory to identify all devices on the network.[32] The component inventory affects the success of other controls, such as vulnerability and patch management. OIT's Cybersecurity Operations Center identifies and reports on threats and vulnerabilities. Vulnerabilities that cannot be remediated by Enterprise Vulnerability Management are assigned to system personnel or the information security officer for action. This process helps to secure devices from attack.

Finding 1: The Northern Arizona VA Healthcare System Had Deficiencies in Four Configuration Management Controls

To assess configuration management controls, the inspection team interviewed the system owner, information system security officer, and system steward. The team reviewed local policies, procedures, and inventory lists and scanned the Northern Arizona VA Healthcare System's network to identify devices. The team compared the devices found on the network with the device inventories provided by VA, received vulnerability lists provided by OIT, and scanned the Northern Arizona VA Healthcare System's network to identify vulnerabilities.[33]

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

[31] GAO, *FISCAM*.

[32] GAO, *FISCAM*.

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

Vulnerability Management and Flaw Remediation

VA has a vulnerability management program, but it can be improved. Prior FISMA audits repeatedly found deficiencies in VA's vulnerability management controls. Consistent with those findings, the team identified deficient controls at the Northern Arizona VA Healthcare System.[34] Vulnerability management is the process by which OIT identifies, classifies, and reduces weaknesses and is part of assessing and validating risks, as well as monitoring the effectiveness of a security program. The Cybersecurity Operations Center identifies and reports on threats and vulnerabilities, and OIT conducts scans for vulnerabilities both routinely and randomly, or when new vulnerabilities are identified and reported.

VA conducts periodic independent scans of all its systems. Discovered vulnerabilities are entered into a plan of action and milestones for remediation by the system steward. System technicians then use the Remediation Effort Entry Form to document mitigation or remediation efforts for each deficiency identified from the scan and provide evidence that the deficiencies have been mitigated.[35]

NIST assigns severity levels to vulnerabilities by using the Common Vulnerability Scoring System, a framework for communicating the characteristics of software vulnerabilities.[36] The scoring system captures the principal characteristics of a vulnerability and produces a numerical score reflecting its severity. Numerical scores are classified as risk levels (low, medium, high, or critical) to help organizations properly assess and prioritize vulnerability management processes. For example, on a scale of zero to 10, critical-risk vulnerabilities have a score between 9.0 and 10, while high-risk vulnerabilities have a score between 7.0 and 8.9. VA requires that critical-risk vulnerabilities be remediated within 30 days and high-risk vulnerabilities be remediated in 60 days.[37]

The inspection team compared OIT-provided network vulnerability scan results from the Northern Arizona VA Healthcare System against its own scans conducted from October 24 to October 28, 2022. The team and OIT used the same vulnerability-scanning tools. The team identified 245 vulnerabilities (112 critical-risk vulnerabilities on 2 percent of the devices and 133 high-risk vulnerabilities on 29 percent of the devices) that were not mitigated within the time

[34] 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."

[35] 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.

[36] "Vulnerability Metrics," NIST National Vulnerability Database, accessed September 29, 2022, 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 September 29, 2022, https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf.

[37] Department of Veterans Affairs Information Security Knowledge Service, "Security Controls Explorer," accessed January 23, 2023 (not accessible by the public). The Information Security Knowledge Service is the approved source for VA cybersecurity and privacy policies, procedures, processes, and guidance.

frames established by OIT. Moreover, OIT's security scans did not identify 83 critical-risk vulnerabilities the team detected.[38] Similarly, the prior FISMA audit found that "VA did not have a complete inventory of all vulnerabilities present on locally hosted systems."[39] The OIG identified critical- and high-risk vulnerabilities on 31 percent of the devices at the Northern Arizona VA Healthcare System. Interviews with personnel responsible for local vulnerability remediation indicated that they prioritize critical-risk vulnerability remediations. The low percentage of critical-risk vulnerabilities supports that claim. While OIT is aware of many of the vulnerabilities, its plans of action and milestones did not list specific vulnerabilities, strategies for remediation, or any resource constraints.[40] 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 healthcare system did not remediate all flaws affecting devices in its network. For example, the inspection team identified vulnerabilities, such as operating systems that were no longer supported by the vendor and applications with missing security patches. The flaw remediation process identifies, reports, and corrects system flaws, including installing security-relevant software and firmware updates.[41] Security-relevant updates include 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

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

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

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

[41] NIST Special Publication 800-53.

used to help alleviate many of the challenges in securing systems from cyberattack, previous FISMA audits have repeatedly found deficiencies in this area.[42]

Unsupported Infrastructure Components

The OIG noted that 71 out of 80 of the Northern Arizona VA Healthcare System's network switches used operating systems that did not meet OIT baseline requirements and 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 components.[43] Additionally, noncurrent software may be vulnerable to malicious code.[44] Network devices and IT systems are critical infrastructure for an organization.[45] Upgrading is not just a defensive strategy but a practical one that protects network stability.

Database Did Not Meet Baseline Configurations

The OIG identified a local database with multiple vulnerabilities caused by configurations that deviated from the OIT security baseline. The baseline is a guide that provides policy, guidance, and implementation of security controls for the database. According to the area manager, the database was added in the background during the installation of an application. Consequently, the database did not have personnel assigned to configure and manage it. After the OIG made the system steward aware of the database, the steward initiated the process of moving the application to the VA Enterprise Cloud, where baseline configurations can be applied and managed by the Database Management Service Line. Data stored in a database has become a more frequent target for malicious users. The impact of such an attack can result in identity theft, financial loss, loss of privacy, a breach of national security, or other types of corruption that can result from unauthorized access to sensitive data. Without managing and applying baseline configuration, OIT is unaware of weaknesses that could adversely impact the database.

Finding 1 Conclusion

The Northern Arizona VA Healthcare System vulnerability management controls did not identify all network weaknesses, such as unsupported versions of applications, and flaw remediation controls did not ensure comprehensive patch management. Further, vulnerabilities were not

---

[42] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2021*; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2020*, Report No. 20-01927-104, April 29, 2021; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2019*, Report No. 19-06935-96, March 31, 2020.

[43] NIST Special Publication 800-53.

[44] GAO, *FISCAM*.

[45] "Silent Risk—Why We Must Upgrade Network Software," Cisco, accessed December 22, 2022, https://www.cisco.com/c/dam/en_us/about/security/cspo/docs/perspective_silent_risk.pdf.

always remediated within time frames established by OIT. Additionally, the Northern Arizona VA Healthcare System network devices were using old operating systems that were no longer supported by the vendor. Finally, there was an unmanaged database that did not have security baseline configurations applied. Without effective configuration management controls, management does not have adequate assurance that the system and network will perform as intended and to the extent needed to support VA's mission.

Recommendations 1–4

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

1. Implement a more effective vulnerability management program to address security deficiencies identified during the inspection.
2. Ensure vulnerabilities are remediated within established time frames.
3. Implement more effective configuration control processes to ensure network devices maintain vendor support.
4. Ensure the unmanaged database completes the transition to the VA Enterprise Cloud where it can be managed and have security baselines applied.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 1 through 4.

In addressing recommendation 1, the assistant secretary reported that VA consistently maintains a 90 percent or greater management rate of critical vulnerabilities across the enterprise. The assistant secretary stated that VA's overall compliance percentages provide evidence that VA has implemented, and is managing, an effective vulnerability management program aligned with industry standards. The assistant secretary also stated that VA's established vulnerability management life cycle encompasses a focus on continuous improvement, including consistent, ongoing reduction of aged vulnerabilities persisting beyond identified remediation timelines, continuous maturity in detection-scanning capabilities, and continuous expansion of visibility, reporting, and tracking of vulnerabilities.

Regarding recommendation 2, the assistant secretary stated VA can provide evidence of remediation of vulnerabilities that persist beyond established remediation time frames and that VA continues to improve plan-of-action and milestones process details, per the VA material-weakness roadmap. The assistant secretary also stated that VA detects and remediates vulnerabilities that persist beyond identified remediation time frames and that are above configuration baselines as part of its standard patch and configuration management program, which includes timelines for testing, packaging, and phased deployment.

Regarding recommendation 3, the assistant secretary reported that upgrades had been completed to ensure baseline requirements were met. For recommendation 4, the assistant secretary stated that the identified equipment had been retired and the service had been moved to the VA Enterprise Cloud.

OIG Response

The assistant secretary reported that corrective actions for recommendations 3 and 4 were complete. The corrective actions are responsive to the intent of the recommendations. Based on evidence provided, the OIG considers those recommendations closed.

Despite concurring with recommendation 1, the assistant secretary reported that VA consistently maintains a management rate of 90 percent or greater for critical vulnerabilities across the enterprise. However, VA did not provide evidence that would allow the OIG to validate this assertion. In fact, OIT's own scan results that the OIG received on April 19, 2023, showed that 57 percent of the critical- and high-risk vulnerabilities had remediations completed, while the remaining vulnerabilities were awaiting updates or had corresponding plans of action and milestones.

The assistant secretary also stated that VA's overall patch and vulnerability compliance percentages provide evidence of an effective vulnerability management and flaw remediation program. However, this statement runs counter to the OIG's results that showed 245 vulnerabilities (112 critical-risk vulnerabilities on 2 percent of the devices and 133 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 83 critical-risk vulnerabilities the OIG detected.

The assistant secretary also concurred with recommendation 2 and stated that VA can provide evidence of remediation of vulnerabilities that persist beyond established remediation time frames. However, VA did not provide evidence that would allow the OIG to validate the claim. The OIG will monitor implementation of the planned actions and close the recommendations when VA provides evidence demonstrating progress in addressing the issues identified. The full text of the response from the assistant secretary is included in appendix D.

II. Security Management Controls

According to FISCAM, security management controls establish a framework and continuous cycle for assessing risk, developing security procedures, and monitoring the effectiveness of the procedures. The inspection team evaluated five security management critical elements: establish a security management program, assess and validate risk, document and implement security control policies and procedures, monitor the effectiveness of the security program, and effectively remediate information security weaknesses.[46]

Finding 2: The Northern Arizona VA Healthcare System Had One Security Management 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 (eMASS), VA's cybersecurity management service for workflow automation and continuous monitoring. Among the topics reviewed were the system security plan, security authorization and risk assessment, security control policies and procedures, and plans of action and milestones for known deficiencies. The team also interviewed the area manager, information system security officer, and facility manager. Finally, the team conducted walk-throughs of the facility.

The OIG found that the Northern Arizona VA Healthcare System has a system security plan and risk assessment that has been documented and approved by management. There are documented security control policies and procedures in place that are signed and approved. The Northern Arizona VA Healthcare System has developed and implemented plans of action and milestones for self-identified weaknesses. The plans of action and milestones have been periodically reviewed. However, the OIG did find a deficiency in continuous monitoring of the inventory at the healthcare system.

Lack of Continuous Monitoring for Inventory

The OIG discovered almost twice the number of devices on the network when compared to those identified in eMASS. Subsequently, OIT provided an inventory of components that was close to those the OIG identified. Consequently, the inspection team determined that OIT is aware of the devices in use but was not routinely updating the inventory in eMASS. Continuous monitoring facilitates ongoing awareness of the system security and privacy posture to support organizational risk management decisions. Frequent updates to hardware and software inventories are a key component of VA's continuous monitoring program. eMASS continuous monitoring reports and metrics provide management with information about the system and its

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

security posture, which in turn supports risk management and authorization decisions. The system owner and steward did not update the inventory in eMASS to accurately reflect hardware located at the facility. By not periodically updating the hardware inventory within eMASS, management is making risk decisions based on inaccurate system information.

Finding 2 Conclusion

The Northern Arizona VA Healthcare System monitoring controls did not identify all components in the healthcare system on a continuous and timely basis. Without effective monitoring controls, VA cannot determine if security controls are designed appropriately and operating effectively, which could lead to management making risk decisions based on inaccurate information.

Recommendation 5

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

5. Implement an improved inventory process to ensure that all connected devices used to support VA programs and operations are documented in the Enterprise Mission Assurance Support Service.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendation 5. In addressing the recommendation, the assistant secretary reported VA has established an integrated product team to review, analyze, and resolve gaps in logical inventory enterprise-wide and will continue to work with the Northern Arizona VA Healthcare System to ensure all connected devices used to support VA program and operations are documented.

OIG Response

The assistant secretary reported that corrective actions for recommendation 5 were in progress. The corrective actions are responsive to the intent of the recommendation. The OIG will monitor implementation of the planned actions and will close the recommendation when VA provides evidence demonstrating progress in addressing the issues identified.

III. 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 controls can be both logical and physical. Logical access controls require users to authenticate themselves, limit the resources users can access, and restrict actions users can take. Physical access controls involve restricting physical access to computer resources and protecting them from loss or impairment. Identification, authentication, and authorization controls ensure that users have the proper access and are uniquely identified. At the Northern Arizona VA Healthcare System, the inspection team reviewed 10 access controls.[47]

Finding 3: The Northern Arizona VA Healthcare System Had Deficiencies in Seven Access Controls

To evaluate the Northern Arizona VA Healthcare System's access controls, the inspection team interviewed the area manager, information system security officer, biomedical equipment supervisor, database administrators, and local IT specialists; reviewed local policies and procedures; and conducted walk-throughs of the facility.[48]

The OIG found these issues with access controls at the Northern Arizona VA Healthcare System:

- Physical access was not effectively controlled.
- Video surveillance for the data center was not installed.
- Several communication rooms containing infrastructure network equipment lacked environmental controls.
- Network infrastructure equipment was improperly installed.
- Uninterruptible power supplies to support network infrastructure equipment were lacking.
- Eleven communication rooms did not have fire-detection or suppression systems.
- Water detection sensors were not installed in the data center.

Physical Access

The OIG discovered multiple communications rooms where physical access was not effectively controlled. Physical access includes devices and barriers to prevent movement from publicly

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

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

accessible areas to nonpublic areas.[49] The healthcare system had an automated physical access control system in which a badge is used to gain entry to buildings and rooms. However, the system was not fully operational. Instead, employees routinely use keys to gain access. A key inventory is required every six months, but an inventory has not been conducted at the facility in more than two years due to locksmith turnover and a failure to accurately track key distribution. The facility manager stated, "People had keys that weren't logged so the logging failed, and we aren't sure who has keys right now." As a result, the facility is replacing the entire key system. On September 30, 2022, a contract was awarded for the new key system. Restricting physical access protects IT resources from loss or impairment.

Video Surveillance

During the facility walk-through, the inspection team discovered that the Northern Arizona VA Healthcare System did not have a video surveillance system for the data center at the Bob Stump VA Medical Center. Video surveillance is the use of cameras installed at strategic locations and is required for data centers.[50] The facility did have camera systems in the patient care buildings. The healthcare system is in the process of upgrading its surveillance system, which would significantly expand its surveillance capability. Ineffective monitoring of activities supporting information systems minimizes the facility's incident response capabilities in the event of a security compromise. The lack of an effective incident response can undermine management's awareness of security vulnerabilities that could hinder the operation of mission-critical systems.

Temperature and Humidity Controls

During walk-throughs, the inspection team discovered several communication rooms without temperature or humidity controls. Environmental controls maintain and monitor temperature and humidity where communication equipment is located.[51] Equipment was installed in communication rooms without sufficient environmental controls. Temperature extremes can cause reduced efficiency and a variety of problems, including premature aging and failure of equipment. High humidity can cause corrosion of internal components and degradation of electrical functionality. This is a risk because insufficient environmental controls can have a significant adverse impact on the availability of systems that are needed to support the organizational mission and business functions.

[49] NIST Special Publication 800-53.

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

[51] NIST Special Publication 800-53.

Improper Equipment Installation

The Northern Arizona VA Healthcare System did not properly install network infrastructure equipment. While VA establishes standards for network equipment installation, the healthcare system did not follow those standards for some equipment. The team identified five instances of network equipment not mounted to equipment racks. Unsecured devices are susceptible to damage, which can interrupt the availability of information to portions of the network serviced by the device. Further, the team found stacked equipment, which impedes proper cooling and can cause premature equipment failure due to overheating.

Emergency Power

The team also found several communication rooms missing uninterruptible power supplies supporting the healthcare system. An uninterruptible power supply is an electrical system or mechanism that provides emergency power when the main power source fails.[52] They are typically used to protect devices, data centers, 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. Without operational uninterruptible power supplies, equipment will not function during power fluctuations or outages, resulting in interruption of data flow and disruption of access to network resources.

Fire Protection

The team discovered 11 communication rooms missing fire-detection or suppression controls. VA requires fire suppression and detection systems, such as sprinkler systems, fire extinguishers, fixed fire hoses, and smoke detectors. Additionally, qualified inspectors must conduct fire protection inspections annually, and the facility must maintain a record of inspections. Without fire-detection and suppression systems, VA would not be able to prevent potential damage to facilities or interruptions in service.

Water Detection

During the walk-through, the team determined that the data center lacked water sensors. When asked, facility staff were unsure whether water sensors were installed. Further, the inspection team was unable to identify water sensors where they should have been located. Water sensors detect the presence of water in a data center and can help minimize damage to equipment due to water leaks. OIT requires facility management and the area manager to be alerted when automated mechanisms detect the presence of water in the vicinity of the information system.

[52] NIST Special Publication 800-53.

Without water sensors, VA would not be able to minimize losses or prevent incidents by detecting leaks early.

Finding 3 Conclusion

The Northern Arizona VA Healthcare System did not control physical access through either the physical access control system or key management. While VA establishes standards for network equipment installation, those standards were not followed for some network equipment, and the data center had no video surveillance camera. Furthermore, several communication rooms did not have temperature or humidity controls, which could have a significant adverse impact on the availability of systems. Uninterruptible power supplies, which protect equipment in case of power outages, were not installed in several communication rooms. Fire-detection and suppression systems, which could prevent potential damage to facilities or interruptions in service, were not installed for 11 communication rooms. Finally, water detection sensors, which could diminish or prevent damage caused by leaks, were not installed in the data center. Unless the healthcare system takes corrective actions, it risks unauthorized access to critical network resources, inability to respond effectively to incidents, and loss of personally identifiable information.

Recommendations 6–11

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

6. Ensure network infrastructure equipment is properly installed.

The OIG made the following recommendations to the Northern Arizona VA Healthcare System director:

7. Ensure physical access controls are implemented for communication rooms.
8. Ensure a video surveillance system is operational and monitored for the data center.
9. Ensure communication rooms with infrastructure equipment have adequate environmental controls.
10. Ensure communication rooms with infrastructure equipment have fire-detection and suppression systems.
11. Ensure water detection sensors are implemented in the data center.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 6 through 11. The assistant secretary reported that work was completed and requested closure for recommendations 6, 9, and 10.

In addressing recommendation 6, the assistant secretary reported that Northern Arizona VA Healthcare System IT personnel properly installed and mounted all network infrastructure equipment. To address recommendation 7, the assistant secretary reported that the healthcare system has awarded a contract to rekey the entire facility, with expected completion in September 2023. The assistant secretary reported that a purchase order has been submitted for installation of a camera system to address recommendation 8. For recommendation 9, the assistant secretary reported that a new system was installed to restrict physical access to equipment. Regarding recommendation 10, the assistant secretary reported that the facility maintenance services team conducted a survey and determined that all in-place equipment met or exceeded the requirements in VA's fire protection design manual. Finally, the assistant secretary stated that the facility maintenance service team is working to ensure water detection sensors are implemented with expected completion in the fourth quarter of 2023.

OIG Response

The assistant secretary reported that corrective actions for recommendations 6, 9, and 10 were complete and requested closure. The corrective actions for 6 and 10 are responsive to the intent of the recommendations. However, the assistant secretary did not provide sufficient evidence to support closure of the recommendations. While the response to recommendation 9 did not address the recommendation, evidence was provided that allowed the OIG to validate that actions had been taken to meet the intent of the recommendation and the OIG considers it closed.

The assistant secretary reported that recommendations 7, 8, and 11 were in progress. The 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.

Appendix A: FISMA Audit for Fiscal Year 2022 Report Recommendations

In the FISMA audit for fiscal year 2022, CliftonLarsonAllen LLP made 26 recommendations. Of these, all 26 were repeat recommendations from the prior year. The FISMA audit assesses the agencywide security management program, and recommendations in the FISMA report are not specific to the Northern Arizona VA Healthcare System. The 26 recommendations are listed below.

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

10. Strengthen processes to ensure appropriate levels of background investigations are completed for applicable VA employees and contractors.
11. Implement more effective automated mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and web application servers.
12. Implement a more effective patch and vulnerability management program to address security deficiencies identified during our assessments of VA's web applications, database platforms, network infrastructure, and workstations.
13. Maintain a complete and accurate security baseline configuration for all platforms and ensure all baselines are appropriately monitored for compliance with established VA security standards.
14. Implement improved network access controls that restrict medical devices from systems hosted on the general network.
15. Enhance procedures for tracking security responsibilities for networks, devices, and components not managed by the Office of Information and Technology to ensure vulnerabilities are remediated in a timely manner.
16. Implement improved processes to ensure that all devices and platforms are evaluated using credentialed vulnerability assessments.
17. Implement improved procedures to enforce standardized system development and change control processes that 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 agencywide incident response procedures to ensure timely notification, reporting, updating, and resolution of computer security incidents in accordance with VA standards.
21. Ensure that systems and applications are adequately logged and monitored to facilitate agencywide awareness of information security events.
22. Implement improved safeguards to identify and prevent unauthorized vulnerability scans on VA networks.

23. Implement improved measures to ensure that all security controls are assessed in accordance with VA policy and that identified issues or weaknesses are adequately documented and tracked within Plans of Action and Milestones.
24. Implement improved processes to monitor for unauthorized changes to system components and the installation of prohibited software on all agency devices and platforms.
25. Develop a comprehensive inventory process to identify connected hardware, software, and firmware used to support VA programs and operations.
26. Implement improved procedures for monitoring contractor-managed systems and services and ensure information security controls adequately protect VA sensitive systems and data.

Appendix B: Background

Federal Information System Controls Audit Manual

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

FISCAM breaks configuration management controls into the following critical elements:

- **Develop and document configuration management policies, plans, and procedures** at the entity, system, and application levels to ensure effective configuration management processes. These procedures should cover employee roles and responsibilities, change control, system documentation requirements, establishment of decision-making structure, and configuration management training.
- **Maintain current configuration information,** which involves naming and describing physical and functional characteristics of a controlled item, as well as performing activities to define, track, store, manage, and retrieve configuration items. Examples of these controls are baseline configurations, configuration settings, and component inventories.
- **Authorize, test, approve, and track changes** by formally establishing a change management process, with management's authorization and approval of the changes. This element includes documenting and approving test plans, comprehensive and appropriate testing of changes, and creating an audit trail to clearly document and track changes.
- **Conduct routine configuration monitoring** to determine the accuracy of the changes that should address baseline and operational configuration of hardware, software, and firmware.[53] 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,

[53] 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.

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

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

FISCAM has seven critical elements for security management:

- **Institute a security management program** that establishes policies, plans, and procedures clearly describing all major systems and facilities and that outlines the duties of those responsible for overseeing security as well as those who own, use, or rely on the organization's computer resources. There should be a clear security management structure for systems and devices as well as for business processes. Examples of specific controls are system security plans, plan updates, activity planning, and resource allocation.
- **Assess and validate risk** by comprehensively identifying and considering all threats and vulnerabilities. This step ensures that agencies address the greatest risks and appropriately decide to accept or mitigate risks. Examples of these controls are security certification, accreditation, categorization, and risk assessment.
- **Document and implement security control policies and procedures** that appropriately address general and application controls and ensure users can be held accountable for their actions. These controls, which are more general at the entity-wide level and more specific at the system level, should be approved by management.
- **Implement security awareness and personnel policies** that provide training for new employees, contractors, and users; periodic refresher training; and distribution of security policies detailing rules and expected behaviors. This element also addresses hiring, transfers, terminations, and performance for employees, contractors, and users. Examples of controls in this area are security awareness training, rules of behavior, position categorization, personnel policies, personnel screening, termination, transfer, access agreements, third-party personnel security, and personnel sanctions.

- **Monitor the program** to ensure that policies and controls effectively reduce risk on an ongoing basis. Effective monitoring involves testing controls to evaluate and determine whether they are appropriately designed and operating effectively. Examples of these controls are security assessments, continuous monitoring, privacy impact assessments, and vulnerability scanning.
- **Remediate information security weaknesses** when they are identified, which involves reassessment of related risks, applying appropriate corrective actions, and follow-up monitoring to ensure actions are effective. Agencies develop plans of actions and milestones to track weaknesses and corresponding corrective actions.
- **Ensure third parties are secure,** as vendors, business partners, and contractors are often granted access to systems for purposes such as outsourced software development or system transactions.[54]

FISCAM lists six access control critical elements:

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

[54] GAO, *FISCAM*.

- **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 are to

- 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; and
- recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.[55]

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

NIST Information Security Guidelines

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

[55] FISMA § 3551.

Appendix C: Scope and Methodology

Scope

The inspection team conducted its work from September 2022 through April 2023. The team evaluated configuration management, security management, and access controls of operational VA IT assets and resources in accordance with FISMA, NIST security guidelines, and VA's IT security policy. In addition, the team assessed the capabilities and effectiveness of IT security controls used to protect VA systems and data from unauthorized access, use, modification, or destruction.

Methodology

To accomplish the objective, the inspection team examined relevant laws and policies. The team also inspected the facility and systems for security compliance. Additionally, the team interviewed VA personnel responsible for the Northern Arizona VA Healthcare System's IT security and operations and privacy compliance. The team conducted vulnerability and configuration testing to determine local systems' security compliance. Finally, the team analyzed the results of testing, interviews, and the inspection to identify 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 information security inspections is the evaluation of general security and application controls that support VA's programs and operations. According to the risk management framework for VA information systems, the information security program is the foundation for VA's information security and privacy program and practices. The framework is documented in VA Handbook 6500.

The team used the GAO's *FISCAM* as a template to plan for inspections. When planning for this review, the team identified potential information system controls that would significantly impact the review. Specifically, the team used *FISCAM* appendix II as a guide to help develop evidence requests and a base set of interview questions for the Northern Arizona VA Healthcare System and its personnel. The team used the *FISCAM* controls identified in appendix B as an overlay to correlate FISMA controls used by VA to protect and secure their information systems. Although similar to the contractor-conducted annual FISMA audits, this review focused on security controls that are implemented at the local level. However, there are some controls that overlap and are assessed in both assessments due to redundant roles and responsibilities among VA's local, regional, and national facilities and offices.

The inspection team determined that all controls applicable to the Northern Arizona VA Healthcare System aligned with the control activities category. Control activities are the actions management establishes through policies and procedures to achieve objectives and respond to risks in the internal control system, which includes the entity's information systems. When the team identified control activity deficiencies, team members assessed whether other relevant controls contributed to those deficiencies. The team did not address risk assessment controls because VA's risk management framework is based on NIST security and privacy controls.

Fraud Assessment

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

Data Reliability

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

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

Government Standards

The OIG conducted this inspection 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: May 10, 2023

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

Subj: OIG Draft Report: Inspection of Information Security at the Northern Arizona VA Healthcare System, Project Number 2022-04104-AE-0171 (VIEWS 10014673)

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 Northern Arizona VA Healthcare System (Project Number 2022-04104-AE-0171).

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 Security at the Northern Arizona VA Healthcare System,
Project Number OIG-2022-04104-AE-0170
(VIEWS 10014673)

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

Comments: Concur.

The Department of Veterans Affairs (VA) Office of Information and Technology (OIT) concurs. VA consistently maintains a 90% or greater management rate of critical vulnerabilities across the enterprise. VA's overall compliance percentages provide evidence that VA has implemented, and is managing, an effective vulnerability management program aligned with industry standards. VA's established vulnerability management lifecycle encompasses a focus on continuous improvement, including consistent, ongoing reduction of aged vulnerabilities persisting beyond identified remediation timelines; continuous maturity in detection-scanning capabilities and continuous expansion of visibility, reporting and tracking of vulnerabilities.

Expected Completion Date: Completed.

VA OIT requests removal or closure of Recommendation 1.

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

Comments: Concur.

VA can provide evidence of remediation of vulnerabilities that persist beyond established remediation timeframes. VA continues to mature its plan of action and milestones (POAM) process for inclusion of related mitigation, business need and roadmap details, per the VA Material Weakness roadmap. VA additionally detects and remediates vulnerabilities that persist beyond identified remediation timeframes and that are above configuration baseline as part of VA's standard patch and configuration management program, which includes timelines for testing, packaging and phased deployment.

Expected Completion Date: Completed.

VA OIT requests removal or closure of Recommendation 2.

Recommendation 3: Implement more effective configuration control processes to ensure network devices maintain vendor support.

Comments: Concur.

The Northern Arizona Healthcare System (HCS) information technology (IT) department made the upgrades required to ensure VA meets OIT baseline requirements on December 15, 2022.

Expected Completion Date: Completed.

VA OIT requests closure of Recommendation 3.

Recommendation 4: Ensure the unmanaged database completes the transition to the VA Enterprise Cloud where it can be managed and have security baselines applied.

Comments: Concur.

VA retired the identified equipment at the Northern Arizona HCS and moved service to the VA Enterprise Cloud on March 17, 2023.

Expected Completion Date: Completed.

VA OIT requests closure of Recommendation 4.

Recommendation 5: Implement an improved inventory process to ensure that all connected devices used to support VA programs and operations are documented in the Enterprise Mission Assurance Support Service.

Comments: Concur.

VA established an enterprise integrated product team to review, analyze and resolve gaps in logical inventory enterprise wide. VA OIT will continue to work with the Northern Arizona HCS to ensure documentation of all connected devices used to support VA programs and operations.

Expected Completion Date: July 31, 2023.

Recommendation 6: Ensure network infrastructure equipment is properly installed.

Comments: Concur.

The Northern Arizona HCS IT personnel properly installed and mounted all network infrastructure equipment on March 17, 2023.

Expected Completion Date: Completed.

VA OIT requests closure of Recommendation 6.

Recommendation 7: Ensure physical access controls are implemented for communication rooms.

Comments: Concur.

The Northern Arizona HCS awarded a contract to rekey the entire facility. The vendor completed the assessment, and work started on September 30, 2022. The Northern Arizona HCS projects all core replacements will be completed within one calendar year.

Expected Completion Date: September 30, 2023.

Recommendation 8: Ensure a video surveillance system is operational and monitored for the data center.

Comments: Concur.

The Northern Arizona HCS issued a purchase order for a camera and installation in accordance with VA Handbook 0730/4, *Security and Law Enforcement*, to minimize potential incidents and enhance response times.

Expected Completion Date: September 30, 2023.

Recommendation 9: Ensure communication rooms with infrastructure equipment have adequate environmental controls.

Comments: Concur.

The Northern Arizona HCS Facility Maintenance Services installed a new system on March 15, 2023. The new system restricts physical access while protecting IT resources from loss or impairment.

Expected Completion Date: Completed.

VA OIT requests closure of Recommendation 9.

Recommendation 10: Ensure communication rooms with infrastructure equipment have fire detection and suppression systems.

Comments: Concur.

The Northern Arizona HCS Facility Maintenance Services team conducted a survey on March 3, 2023, which determined that all in-place equipment either met or exceeded the requirements as indicated in VA's Fire Protection Design Manual. In addition, the areas protected already have the required smoke detection systems in place.

Expected Completion Date: Completed.

VA OIT requests closure of Recommendation 10.

Recommendation 11: Ensure water detection sensors are implemented in the data center.

Comments: Concur.

The Northern Arizona HCS Facility Maintenance Services team is working to ensure water detection sensors are implemented; work is scheduled to be completed in the fourth quarter of fiscal year 2023.

Expected Completion Date: September 30, 2023.

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

OIG Contact and Staff Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Inspection Team	Michael Bowman, Director Ginalynn Alvarado Jack Henserling Shawn Hill Kimberly Moss Adam Sowells
Other Contributors	Bill Warhop Rashiya Washington

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, Northern Arizona VA Healthcare System

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Accountability
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget
US Senate: Mark Kelly, Kyrsten Sinema
US House of Representatives: Andy Biggs, Juan Ciscomani, Elijah Crane, Ruben Gallego, Paul Gosar, Raul Grijalva, Debbie Lesko, David Schweikert, Greg Stanton