DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS HEALTH ADMINISTRATION

Inspection of Information Security at the Southern Oregon Rehabilitation Center and Clinics

INFORMATION SECURITY INSPECTION | REPORT #22-01836-12 | JANUARY 18, 2023

MISSION

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

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

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

www.va.gov/oig/hotline

1-800-488-8244

Executive Summary

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

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

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

The OIG conducted this inspection to determine whether the Southern Oregon Rehabilitation Center and Clinics (SORCC) was meeting federal security guidance. The OIG selected the facility because it had not been previously visited as part of the annual FISMA audit. The inspection scope and methodology are described in appendix C.

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

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

[1] Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014) § 3555(b)(1).

[2] NIST Special Publication 800-53, *Security and Privacy Controls for Federal 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 2021*, Report No. 21-01309-74, April 13, 2022.

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

[5] Government Accountability Office (GAO), *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G, February 2009, p. 12.

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

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

What the Inspection Found

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

Configuration Management Controls Had One Deficiency

The SORCC's configuration management controls had one deficiency in vulnerability management: the process used by Office of Information and Technology (OIT) to identify, classify, and remediate weaknesses.

The OIG determined that OIT's process to remediate identified vulnerabilities needs improvement. OIT scans for vulnerabilities routinely, randomly, and when new vulnerabilities are identified and reported. The inspection team and OIT used the same vulnerability-scanning tools. The inspection team identified 92 vulnerabilities—24 critical vulnerabilities on less than 1 percent of the computers and 68 high-risk vulnerabilities on over 9 percent of the computers—that were previously identified by OIT but were not mitigated within the required 30- or 60-day windows. These vulnerabilities included software and operating systems not supported by the vendor. The oldest vulnerability was identified on the network in 2017.

Without an effective vulnerability management program, vulnerabilities such as security and functionality problems in software and firmware might not be mitigated, increasing opportunities for exploitation.

[6] *FISCAM*, p. 12.
[7] *FISCAM*, p. 11.
[8] *FISCAM*, p. 11.

Security Management Controls Had One Deficiency

The one security management control deficiency was in system security planning, which provides for implementation of security controls to satisfy system requirements and is needed for authorizing a system to operate. Specifically, the OIG determined that the SORCC's special-purpose system, which included segments that contain vulnerable devices, did not have an authorization to operate because it had not cleared the NIST risk management framework process, nor did it have an approved system security plan.[9] The OIG identified four devices in the facility's climate control system connected to the special-purpose system that were using a vulnerable unsupported operating system and were owned and maintained by a contractor.[10] The OIG was provided a copy of the contract that did not include language to require the contractor to adhere to federal and VA security requirements.

Without a system security plan or an authorization to operate, and without requiring contractors to adhere to federal and VA security requirements, the facility cannot be sure that security controls will be implemented as required. A compromise of the climate control system could cause a loss of air-conditioning or heating and threaten the safety of patients, staff members, and visitors.

Five Access Controls Had Deficiencies

The SORCC had security deficiencies in network segmentation, physical access, environmental, audit and monitoring, and records management controls.[11]

The SORCC did not have segmentation controls in place for eight network segments containing medical systems.[12] The inspection team identified eight network segments containing 26 medical computers or devices that did not apply access control lists needed for protection. Without effective network segmentation controls in place, any user can access these potentially vulnerable medical systems. A breach could have a negative impact on the functionality and safety of the medical system.

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

[10] These devices were used to provide heating and air conditioning to SORCC.

[11] NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011, includes updates as of October 10, 2019; VA Handbook 6500, *Risk Management Framework for VA Information Systems: VA Information Security Program*, February 2021.

[12] Network segmentation controls regulate where information can travel within a system and between systems. Network-connected medical devices and special-purpose systems are placed on isolated network segments for protection.

The SORCC did not adequately restrict access to its computer rooms, communication closets, and generators. The team found 12 individuals who could use their access card to enter these areas but were not listed in the access authorization memos for the computer room, including an area manager who had passed away a year before the team's visit. Further, the OIG found the doors for the enclosures housing the facility's two main generators were unlocked. While these two enclosures were fenced in, the fence was unlocked and had barbed wire only on three of the four sides. By not adequately restricting access to these areas, the SORCC is placing IT assets at risk of accidental or intentional destruction.

The team identified the following missing computer room environmental controls:

- Seven communication closets did not contain electrical grounding for equipment.
- Seven communication closets did not have temperature- and humidity-monitoring controls.
- Eleven communication closets and one power building did not have fire suppression systems.
- The police room did not have a smoke detector.

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

The inspection team also identified deficiencies in logging administrative actions, log retention, and log reviews for databases. Specifically, staff could not provide excerpts of logs documenting administrative access to databases at the center. Without this information, security incident investigations may be limited or unsuccessful in determining the unauthorized use or modification of sensitive information.

Finally, during a tour of the facility, the team located several boxes of federal records inside and outside a partially enclosed wire mesh cage within a widely accessible building. The team found that six of the boxes held documents that contained personally identifiable information belonging to 127 individuals and protected health information belonging to 18 of the 127 individuals. Breaches of that information may result in loss of public trust, legal liability, or remediation costs.

What the OIG Recommended

The OIG made a total of nine recommendations, including four to the assistant secretary for information and technology and chief information officer, one to the branch chief of Network Contracting Office 20, and four to the SORCC director.[13]

Recommendations 1, 2, 4, and 5 were directed to the assistant secretary for information and technology and chief information officer: (1) implement a vulnerability management program that ensures timely system changes, (2) develop and approve a system security plan and authorization to operate for the special-purpose system, (4) verify that access controls have been applied to network segments that contain medical systems, and (5) develop and implement a process to retain database logs consistent with VA's record retention policy. The OIG made these recommendations to the assistant secretary because they are related to enterprise-wide information security issues, such as those identified on previous FISMA audits and information security inspections. The OIG directed recommendation 3—to include language for contractors to follow federal or VA information security requirements in contracts that have an IT component—to Network Contracting Office 20's branch chief.

The SORCC director received the remaining four recommendations: (6) develop and implement controls to remove an individual's access rights to computer rooms when access is no longer necessary, (7) implement a process to regularly review applicable reports to ensure that only authorized individuals have computer room access and update the access authorization memo to include only those individuals authorized to have access, (8) validate that appropriate physical and environmental security measures are implemented and functioning as intended, and (9) inventory and verify that records containing personal information are adequately secured.

VA Comments and OIG Response

The assistant secretary for information and technology and chief information officer provided comments for all nine recommendations, including concurrences with eight of them. The assistant secretary did not concur with recommendation 4—to verify that access control lists have been applied to network segments that contain medical systems—reporting that the devices within the network segments do not meet the definition of devices requiring isolation, as defined by VA's Office of Information Security. However, the eight network segments in question were identified by the facility as containing medical systems—including Vista Imaging, Telehealth, medical devices, and equipment used for sterile processing—which, per VA policy, fall under

[13] Network Contracting Office 20 provides procurement support to VHA facilities within the VA Northwest Health Network (Veterans Integrated Service Network 20), including the SORCC.

the medical device isolation architecture guidance and should have access control lists applied.[14] VA policy covers these medical devices that are on the VA network and store sensitive patient information.[15] Therefore, the OIG stands by its recommendation and it will remain open.

The assistant secretary concurred with recommendation 1 but reported that VA's latest analysis of OIG's scan results displayed a 99.88 percent rate of policy compliance. However, no evidence was provided that would allow the OIG to validate this assertion. In fact, OIT's own scan results that the OIG received on November 16, 2022, showed that 48 percent of the critical- and high-risk vulnerabilities had remediation actions completed, while the remaining vulnerabilities were awaiting updates or had corresponding plans of actions and milestones. The assistant secretary also stated VA's overall patch and vulnerability compliance percentages provide evidence that an effective vulnerability management and flaw remediation program has in fact been implemented. The assistant secretary's statement runs counter to the OIG's results, which showed 92 vulnerabilities (24 critical-risk vulnerabilities on less than 1 percent of the devices and 68 high-risk vulnerabilities on 9 percent of the devices) that were not mitigated within the times established by OIT.

The assistant secretary provided responsive action plans for recommendation 1, as well as for recommendations 2 and 8, and the OIG will monitor the implementation of the planned actions and close these recommendations when VA provides sufficient evidence demonstrating progress in addressing the issues identified. Finally, the assistant secretary requested that recommendations 5, 6, 7, and 9 be closed due to corrective actions he said were completed. Based on the evidence provided by the assistant secretary, the OIG considers these four recommendations closed. The full text of the assistant secretary's response is included in appendix D.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

[14] VA Directive 6550, *Pre-procurement Assessment and Implementation of Medical Devices/Systems*, June 3, 2019, p. 15. The imaging system captures clinical images, scanned documents, motion video and other non-text data, and makes them part of the patient's electronic medical record. The telehealth system provides patients within home real-time interactive video visits, remote health monitoring, and devices that gather and store health data.

[15] VA Directive 6550, p. 1.

Contents

Abbreviations

FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
GAO	Government Accountability Office
IT	information technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information and Technology
OMB	Office of Management and Budget
SORCC	Southern Oregon Rehabilitation Center and Clinics

Introduction

Information technology (IT) controls protect VA systems and data from unauthorized access, use, modification, or destruction. To determine compliance with the Federal Information Security Modernization Act of 2014 (FISMA), the VA Office of Inspector General (OIG) contracts with an independent public accounting firm that conducts an annual audit of VA's information security program and practices.[16] The FISMA audit is conducted in accordance with guidelines issued by the Office of Management and Budget (OMB) and applicable National Institute of Standards and Technology (NIST) information security guidelines.[17]

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.[18] 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.[19] Appendix C provides more detail on the inspection scope and methodology.

The OIG conducted this inspection to determine whether the Southern Oregon Rehabilitation Center and Clinics (SORCC) was meeting federal security guidance. The OIG selected the SORCC 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 SORCC, other facilities across VA could benefit from reviewing this information and considering these recommendations.

Security Controls

FISMA was established, in part, to improve oversight of federal agency information security programs. The law requires VA to develop, document, and implement an agencywide information security and risk management program. FISMA also requires the chief information officers and other senior agency officials to report annually on the effectiveness of the agency's

[16] Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014), § 3555(b)(1).

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

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

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

information security program. In addition, FISMA states that inspectors general are required to conduct annual independent evaluations of their respective agencies' information security programs.[20]

Both OMB and NIST provide criteria to evaluate security controls. These criteria provide requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system.[21]

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

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

Table 1. Security Controls Evaluated by the OIG

Control area	Purpose	Examples evaluated
Configuration management	Identify and manage security features for all hardware and software components of an information system	Component inventory, baseline configurations, configuration settings, change management, vulnerability management, and flaw remediation
Contingency planning	Provide reasonable assurance that information resources are protected and risk of unplanned interruptions is minimized, as well as provide for recovery of critical operations should interruptions occur	Continuity of operations, contingency planning, disaster recovery, and environmental safeguards
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

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

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

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

Control area	Purpose	Examples evaluated
Access	Provide reasonable assurance that computer resources are restricted to authorized individuals	Access, identification, authentication, audit, and accountability, including related physical security controls

Source: VA OIG analysis.

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

Office of Information and Technology Structure and Responsibilities

The assistant secretary for information and technology and chief information officer leads the Office of Information and Technology (OIT). According to VA, OIT delivers available, adaptable, secure, and cost-effective technology services to VA and acts as a steward for VA's IT assets and resources. The Cybersecurity Operations Center, 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. Figure 1 shows the organization of offices within OIT that are relevant to this inspection.

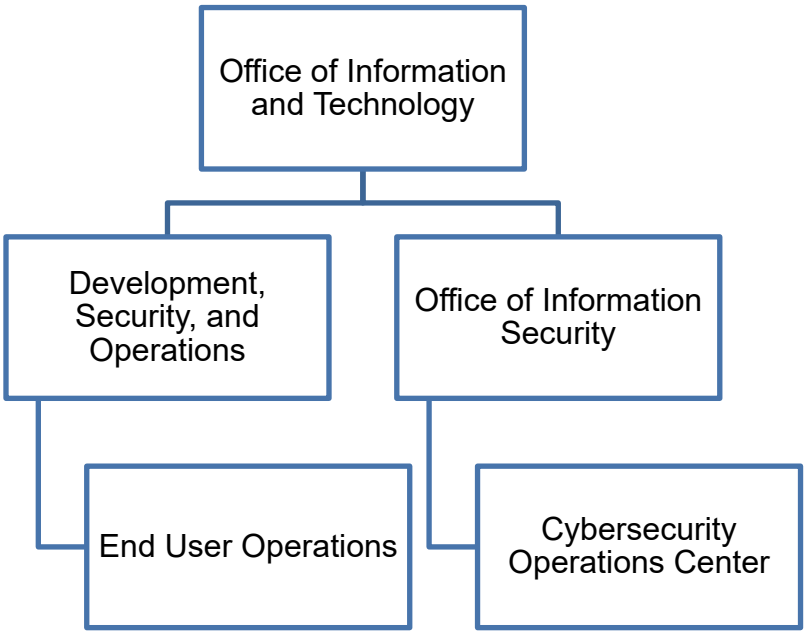

Figure 1. *Organizational structure of OIT entities relevant to this inspection.*
Source: VA OIG analysis.

End User Operations provides onsite and remote support to IT customers across all VA administrations and special program offices, including direct support of over 340,000 VA employees and thousands of contractors who are issued government-furnished IT equipment and access. End User Operations provisions computing devices; conducts new facility activations; performs moves, adds, and changes; executes local system implementations; and engages VA's customers across the nation to meet IT support needs. OIT assigns dedicated End User Operations personnel to the SORCC.

Results of Previous Projects

As previously mentioned, the OIG issues annual reports on VA's information security program. The FISMA audit is conducted in accordance with guidelines issued by OMB and applicable NIST information security guidelines.[23] The fiscal year (FY) 2021 FISMA audit, conducted by CliftonLarsonAllen LLP, an independent public accounting firm, evaluated 50 major applications and general support systems hosted at 24 VA facilities, including the testing of selected management, technical, and operational controls outlined by NIST.[24] CliftonLarsonAllen LLP made 26 recommendations, listed in appendix A. Of these recommendations, all 26 are repeated from the prior annual audit, indicating that VA continues to face significant challenges in complying with FISMA requirements.[25] Repeat recommendations included addressing deficiencies in configuration management, contingency planning, security management, and access controls.

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

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

[23] NIST Special Publication 800-53.

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

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

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

- 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 systems will remain at risk of disruption."[27]

Southern Oregon Rehabilitation Center and Clinics

The SORCC is part of the VA Southern Oregon Healthcare System. The facility saw 16,290 unique outpatients in FY 2021. It also operates a 181-bed capacity mental health residential rehabilitation treatment program. The facility has about 800 full-time employees and a budget of $249 million for FY 2022.[28]

Figure 2. *Southern Oregon Rehabilitation Center and Clinics.*
Source: Southern Oregon Rehabilitation Center and Clinics public affairs officer, January 15, 2020.

[27] GAO, *Information Security: VA and Other Federal Agencies Need to Address Significant Challenges*.
[28] This includes the Office of Community Care.

Results and Recommendations

I. Configuration Management Controls

Configuration management involves identifying and managing security features for all hardware, software, and firmware components of an information system at a given point and systematically controlling changes to that configuration during the system's life cycle.[29] The inspection team reviewed and evaluated the 14 configuration management controls drawn from NIST criteria for VA-hosted systems at the SORCC to determine if they met federal guidance and VA requirements.

An effective configuration management process should be described in a configuration management plan and implemented according to the plan.[30] VA should first establish an accurate component inventory to identify all devices on the network.[31] The component inventory affects the success of other controls, such as vulnerability and patch management. OIT's Cybersecurity Operations Center identifies and reports threats and vulnerabilities for VA. Once this process is complete, OIT's Patch and Vulnerability Team develops procedures to remediate the identified issues, which can include applying patches. This process helps secure devices from attack.

Finding 1: The SORCC Had One Configuration Management Control Deficiency

To assess configuration management controls, the inspection team interviewed the systems owner, information system security officer, and system stewards. The team reviewed local policies, procedures, inventory lists, and network device configurations. The OIG also performed scans of the SORCC's network to identify devices and vulnerabilities. The team compared the devices found on the network with the device inventories and the vulnerability lists provided by OIT.[32] The SORCC's configuration management controls had one deficiency in vulnerability management: the process used by OIT to identify, classify, and remediate weaknesses.

Vulnerability Management

Prior FISMA audits repeatedly found deficiencies in VA's vulnerability assessments. Consistent with those findings, the team identified weaknesses in vulnerability management at the SORCC. According to GAO, "vulnerability assessments involve analyzing a network to identify potential vulnerabilities that would allow unauthorized access to network resources, simulating what

[29] *FISCAM*, p. 268.

[30] *FISCAM*, p. 270.

[31] NIST Special Publication 800-53.

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

might be performed by someone trying to obtain unauthorized access."[33] Vulnerability management is the process by which OIT identifies, classifies, and remediates weaknesses, and is part of assessing and validating risks as well as monitoring the effectiveness of a security program. The Cybersecurity Operations Center identifies and reports on threats and vulnerabilities, and while OIT conducts scans for vulnerabilities, both routinely and randomly, or when new vulnerabilities are identified and reported.[34]

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

Discovered vulnerabilities are entered into a plan of action and milestones for remediation by the system owner. The information system owner or system steward utilizes the Remediation Effort Entry Form to document mitigation or remediation efforts for each deficiency identified from the scan and provides evidence that the deficiencies have been mitigated within established deadlines, based on severity of the vulnerability: 30 days for critical-risk vulnerabilities and 60 days for high-risk ones.

The inspection team compared OIT's vulnerability scan results from the SORCC with scans the inspection team conducted from April 11–14, 2022. OIT and the team used the same vulnerability-scanning tools. The inspection team identified 92 vulnerabilities—24 critical vulnerabilities on less than 1 percent of the computers and 68 high-risk vulnerabilities on 9 percent of the computers—that OIT had identified but not mitigated on time as required. These vulnerabilities included software and operating systems that are not supported by the vendor. The oldest vulnerability was identified on the network in 2017. Similarly, the prior FISMA audit found that "VA did not have a complete inventory of all vulnerabilities present on locally hosted systems."[35] Without an effective vulnerability management program, vulnerabilities such as security and functionality problems in software and firmware might not be mitigated, increasing opportunities for exploitation.

The center did not remediate all flaws affecting devices in its network. Specifically, the inspection team identified unsupported versions of applications and missing patches. The flaw remediation process identifies, reports, and corrects system flaws, which includes installing security-relevant software and firmware updates. Security patches are usually the most effective way to mitigate software flaw vulnerabilities. According to GAO, a patch is a piece of software

[33] *FISCAM*, p. 185.

[34] VA Directive 6500, *VA Cybersecurity Program*, February 24, 2021.

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

code inserted into a program to temporarily fix a defect.[36] NIST further explains that patches correct security and functionality problems in software and firmware.[37] Patch management is how an organization acquires, tests, applies, and monitors updates that address security and functionality problems. Although patch management is a critical process used to help alleviate many of the challenges in securing systems from cyberattack, previous FISMA audits have repeatedly found deficiencies in this area.[38]

Finding 1 Conclusion

The SORCC vulnerability management controls did not ensure vulnerabilities were remediated by VA-established deadlines, creating a risk that they may be exploited. Without effective configuration management, users do not have adequate assurance that the system and network will perform as intended and to the extent needed to support their missions.

Recommendation 1

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

1. Implement a vulnerability management program that ensures system changes within established deadlines.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendation 1, reporting that VA consistently maintains a 90 percent or greater management rate of critical-risk vulnerabilities across the enterprise and that VA's latest analysis of OIG's scan results for the SORCC displayed policy compliance exceeding 99 percent. The assistant secretary indicated VA will follow up on remaining pending or status update vulnerability items to ensure those vulnerabilities are made compliant.

OIG Response

The assistant secretary reported that corrective actions for recommendation 1 were in progress and provided an estimated completion date. The planned corrective actions are responsive to the intent of the recommendation. While the assistant secretary concurred with recommendation 1, he stated that VA's latest analysis of OIG's scan results displayed a 99.88 percent rate of policy

[36] *FISCAM*, p. 136.

[37] NIST Special Publication 800-53.

[38] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2021*; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2020*; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2019*, Report No. 19-06935-96, March 31, 2020; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2018*, Report No. 18-02127-64, March 12, 2019.

compliance. However, OIT's scan results that were provided to the OIG on November 16, 2022, showed that 48 percent of the critical- and high-risk vulnerabilities had remediation actions completed, while the remaining vulnerabilities were awaiting updates or had corresponding plans of actions and milestones. The assistant secretary also stated VA's overall patch and vulnerability compliance percentages provide evidence that an effective vulnerability management and flaw remediation program has already been implemented. The assistant secretary's statement runs counter to the inspection team's results that showed 92 vulnerabilities (24 critical-risk vulnerabilities on less than 1 percent of the devices and 68 high-risk vulnerabilities on 9 percent of the devices) that were not mitigated within the times established by OIT. The OIG will monitor implementation of the planned actions and will close the recommendation when VA provides sufficient evidence demonstrating progress in addressing the issues identified. The full text of the assistant secretary's response is included in appendix D.

II. Contingency Planning Controls

Contingency planning controls are important because if they are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. To determine whether recovery plans will work as intended, they should be tested periodically in disaster-simulation exercises. FISMA requires that each federal agency implement an information security program that includes "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."[39] Although often referred to as disaster recovery or contingency plans, controls to ensure service continuity should address the entire range of potential disruptions. These may include minor interruptions, such as temporary power failures, as well as fires, natural disasters, and terrorism, which would require reestablishing operations at a remote location. To determine if the SORCC met federal guidance and VA requirements, the inspection team evaluated six contingency planning controls.

Finding 2: The SORCC Had No Contingency Planning Control Deficiencies

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

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

[39] FISMA § 3554(b)(8).

III. Security Management Controls

Security management controls establish a framework and continuous cycle for assessing risk, developing security procedures, and monitoring the effectiveness of the security procedures. The inspection team evaluated two security management critical elements: instituting a security management program and assessing and validating risk.[40]

Finding 3: The SORCC Had One Security Management Control Deficiency

To assess security controls, the inspection team reviewed local security management policies and standard operating procedures, as well as applicable VA policies, including documentation from the Enterprise Mission Assurance Support Service, VA's cybersecurity management service for workflow automation and continuous monitoring. Among the topics reviewed were handling of external media, risk analysis, and plans of action and milestones for known deficiencies. The team also conducted a walk-through of the facility and interviewed information system security officers, local administrators, contracting officer's representatives, privacy officers, and system stewards.

System Authorization

The one security management control deficiency was in system security planning, which provides for implementation of security controls to satisfy system requirements and is needed for authorizing a system to operate. The OIG determined that the SORCC's special-purpose system, which included segments that contain vulnerable devices, did not have an authorization to operate because it had not cleared the NIST risk management framework process, nor did it have an approved system security plan.[41] Without an approved security plan and authorization to operate, there are no approved security controls for devices operating on the system. The OIG identified four devices in the facility's climate control system connected to the special-purpose system that were using a vulnerable unsupported operating system and were owned and maintained by a contractor.[42] Though switches restricted the potential exploitation of vulnerabilities on the special-purpose system network segments to computers within the SORCC's user network, without a system security plan or authorization to operate, there is no documentation of acceptance of vulnerability risks. The OIG was provided a copy of the contract, which did not include language requiring the contractor to adhere to federal and VA

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

[41] OIS, System Security Support, SPS Vulnerability Patch Management SOP states: "A Special Purpose System (SPS) is a non-medical, network-connected system that supports building safety, security, and/or environmental controls and cannot obtain a VA-approved baseline configuration due to vendor-controlled system policies, proprietary software, and other system-specific controls and configurations."

[42] These HVAC devices were used to provide heating and air conditioning to the SORCC.

security requirements. Federal and VA security requirements indicate that contractors must adhere to them.[43]

Without a system security plan or an authorization to operate, and without requiring contractors to adhere to federal and VA security requirements, the facility cannot be sure that security controls will be implemented as required. A compromise of the climate control system could cause a loss of air-conditioning or heating and threaten the safety of patients, staff members, and visitors.

Finding 3 Conclusion

The SORCC security management controls did not ensure systems included controls that reduced the risk of loss of confidentiality, integrity, and availability to a level that management accepts. Without effective security management, users do not have adequate assurance that the system and network will perform as intended and to the extent needed to support their missions.

Recommendations 2–3

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

2. Develop and approve a system security plan and an authorization to operate for the special-purpose system.

The OIG made the following recommendation to the branch chief of the Network Contracting Office 20:[44]

3. Include language for contractors to follow federal and VA information technology security requirements in contracts that have an information technology component.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 2 and 3 and reported that VA is developing a system security plan and completing an authority to operate for the special-purpose system. In addition, the assistant secretary reported that VA submitted a contract modification to ensure the relevant Federal Acquisition Regulation clause is included in contracts that have an information technology component.

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

[44] Network Contracting Office 20 provides procurement support to VHA facilities within the VA Northwest Health Network (Veterans Integrated Service Network 20), including the SORCC.

OIG Response

The assistant secretary reported corrective actions for recommendations 2 and 3 are in progress and provided estimated completion dates. The planned corrective actions are responsive to the intent of the recommendations. The OIG will monitor the implementation of the planned actions and will close the recommendations when VA provides sufficient evidence demonstrating progress in addressing the issues identified. The full text of the assistant secretary's response is included in appendix D.

IV. Access Controls

Previous FISMA reports have repeatedly identified access controls as a nationwide issue for VA. Access controls, including boundary protections, sensitive system resources, physical security, and audit and monitoring controls, provide reasonable assurance that computer resources are restricted to authorized individuals. Identification, authentication, and authorization controls ensure that users have the proper access and are uniquely identified. At the SORCC, the inspection team reviewed six critical access control elements.[45]

Finding 4: The SORCC Had Five Access Control Deficiencies

To evaluate the SORCC's access controls, the inspection team interviewed the information system security officer, system stewards, local administrators, and the system owner; reviewed local policies and procedures; conducted walk-throughs of the SORCC; and analyzed audit logs.[46]

The OIG found these issues with access controls at the SORCC:

- Network segmentation controls were missing for eight network segments that contained medical systems.[47]
- Physical access to computer rooms, communication closets, and generators was not adequately restricted.
- Environmental controls were not fully implemented in certain computer rooms and communications closets, including grounding for electrical equipment, monitoring of temperature and humidity, and fire detection and suppression systems.
- Database managers did not adequately maintain log data for local databases.
- Federal records were not properly managed and safeguarded throughout their life cycles.

Network Segmentation

System segmentation controls logically separate and restrict network communication between network segments to protect sensitive systems from unauthorized access. VA provides network segmentation protection through access control lists. However, during the inspection, the OIG identified eight network segments containing 26 medical computers or devices that did not have

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

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

[47] Network segmentation controls regulate where information can travel within a system and between systems. Network connected medical devices and special-purpose systems are placed on isolation network segments for protection.

access control lists applied to restrict system access. Without effective network segmentation controls in place, any user can access these potentially vulnerable medical systems. A compromised medical system could allow a malicious attacker to obtain protected health information or modify the medical system to adversely impact its functionality or safety.

Physical Access

Physical access is the process used to restrict individuals' ability to enter computer rooms and communication closets to protect computer resources from intentional or unintentional loss or impairment.[48] The SORCC did not adequately restrict access to its computer rooms, communication closets, and generators. The team found 12 individuals who could use their access cards to enter these areas but were not listed in the access authorization memos for the computer room. These 12 individuals included one who had passed away a year before the inspection team's visit. Further, the OIG found the doors for the enclosures housing the facility's two main generators were unlocked. While these two enclosures were fenced in, the fences were unlocked and there was only barbed wire on three of the four sides. By not adequately restricting access to these areas, the SORCC is placing IT assets at risk of accidental or intentional destruction.

Environmental Controls

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

- Seven communication closets did not contain electrical grounding for equipment.
- Seven communication closets did not have temperature- and humidity-monitoring controls.
- Eleven communication closets and the power building did not have fire suppression systems (fire extinguishers or water sprinklers).
- The police room did not have a smoke detector.

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

Audit and Monitoring

Audit and monitoring provide for the collection, review, and analysis of events for indications of inappropriate or unusual activity. The OIG determined that improvements are needed for logging administrative actions, log retention, and log reviews for databases at the SORCC. Audit and

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

monitoring controls should be routinely used to assess the effectiveness of security controls, and to recognize and investigate attacks.[49] OIT was unable to provide the OIG with database log files from databases located at the SORCC. If this information is not available, an investigation may be limited or unsuccessful in determining the unauthorized use or modification of information.

Records Management

The facility's Records Management Program did not appropriately manage and safeguard federal records throughout their life cycles. During a tour of the facility, the team located several boxes inside and outside a partially enclosed wire mesh cage within a widely accessible building. The team found that six of the boxes held documents that contained personally identifiable information belonging to 127 individuals and protected health information belonging to 18 of them. Breaches of that information may result in loss of public trust, legal liability, or remediation costs.

Finding 4 Conclusion

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

Recommendations 4–9

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

4. Verify that access control lists have been applied to network segments that contain medical systems.
5. Develop and implement a process to retain database logs for a period consistent with VA's record retention policy.

The OIG made the following recommendations to the Southern Oregon Rehabilitation Center and Clinics director:

6. Develop and implement controls to remove an individual's access rights to computer rooms when access is no longer necessary.
7. Implement a process to regularly review applicable reports to ensure that only authorized individuals have computer room access and update the system access

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

authorization memo to include only those individuals necessary to perform job functions.

8. Validate that appropriate physical and environmental security measures are implemented and functioning as intended.
9. Inventory and verify that records containing personally identifiable information and personal health information are adequately secured.

VA Management Comments

The assistant secretary for information and technology did not concur with recommendation 4, stating that the devices within the network segments do not meet the definition of devices requiring isolation as defined by the Office of Information Security. The assistant secretary concurred with recommendations 5 through 9, reporting that VA, in response to these recommendations, has since corrected the issue for retaining database logs; implemented a visitor log to track and control access to computer rooms; modified access controls to the OIT-controlled access areas; initiated work orders to ensure that all appropriate physical and environmental security measures are implemented and functioning properly; and secured the records identified by OIG in accordance with VA and Veterans Health Administration incident response procedures. The assistant secretary requested that recommendations 5, 6, 7, and 9 be closed due to corrective actions he said were completed.

OIG Response

Regarding recommendation 4, the eight network segments noted by the OIG were identified by the facility as containing medical systems, including Vista Imaging, Telehealth, medical devices, and equipment used for sterile processing.[50] Per VA policy, these devices would fall under the medical device isolation architecture guidance and should have access control lists applied.[51] VA policy covers these medical devices that are on the VA network and store sensitive patient information.[52] Therefore, the OIG stands by its recommendation.

For recommendations 5, 6, 7, 8, and 9, the planned corrective actions are responsive to the intent of the recommendations. Based on the evidence provided by the assistant secretary, the OIG considers recommendations 5, 6, 7, and 9 closed. The OIG will monitor the implementation of the planned actions related to recommendation 8 and will close the recommendation when VA

[50] VA Directive 6550, *Pre-procurement Assessment and Implementation of Medical Devices/Systems*, June 3, 2019, p. 15. The imaging system captures clinical images, scanned documents, motion video and other non-text data, and makes them part of the patient's electronic medical record. The telehealth system provides patients with in-home real-time interactive video visits, remote health monitoring, and devices that gather and store health data.

[51] VA Directive 6500.

[52] VA Directive 6550, p. 1.

provides sufficient evidence demonstrating progress in addressing the issues identified. The full text of the assistant secretary's response is included in appendix D.

Appendix A: FISMA Audit for FY 2021 Report Recommendations

In the FISMA audit for FY 2021, CliftonLarsonAllen LLP made 26 recommendations. All 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 SORCC. The 26 recommendations are listed below.

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

11. Implement more effective automated mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and web application servers.
12. Implement a more effective patch and vulnerability management program to address security deficiencies identified during our assessments of VA's web applications, database platforms, network infrastructure, and workstations.
13. Maintain a complete and accurate security baseline configuration for all platforms and ensure all baselines are appropriately implemented for compliance with established VA security standards.
14. Implement improved network access controls that restrict medical devices from systems hosted on the general network.
15. Consolidate the security responsibilities for networks not managed by the Office of Information and Technology, under a common control for each site and ensure vulnerabilities are remediated in a timely manner.
16. Implement improved processes to ensure that all devices and platforms are evaluated using credentialed vulnerability assessments.
17. Implement improved procedures to enforce standardized system development and change control processes that 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 VA's Cybersecurity Operations Center has full access to all security incident data to facilitate an 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. Fully develop a comprehensive list of approved and unapproved software and implement continuous monitoring processes to prevent the use of prohibited software on agency devices.
25. Develop a comprehensive inventory process to identify connected hardware, software, and firmware used to support VA programs and operations.
26. Implement improved procedures for monitoring contractor-managed systems and services and ensure information security controls adequately protect VA sensitive systems and data.

Appendix B: Background

Federal Information System Controls Audit Manual

GAO developed the Federal Information System Controls Audit Manual (FISCAM) to provide auditors and information system control specialists with 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, and identification of other emerging threats. Software releases should be controlled to prevent

[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.

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 identifies the following critical elements for contingency planning:

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

FISCAM has seven critical elements for security management:

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

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

[54] *FISCAM*, p. 194.

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

Federal Information Security Modernization Act of 2014

The stated goals of FISMA are the following:

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

[55] FISMA.

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

NIST Information Security Guidelines

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

Appendix C: Scope and Methodology

Scope

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

Methodology

To accomplish the objective, the inspection team examined relevant laws and policies. The team also inspected the facility and systems for security compliance. Additionally, the team interviewed VA personnel responsible for the SORCC'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 IT security inspections is the evaluation of general security and application controls that support VA's programs and operations. According to the risk management framework for VA information systems, the information security program is the foundation for VA's information security and privacy program and practices. The framework is documented in VA Handbook 6500.

The team used the 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 SORCC 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 its information systems. Although similar to the contractor-conducted annual FISMA audits, this review focused on security controls that are implemented at the local level. However, there are some controls that overlap and are 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 SORCC aligned with the control activities category. Control activities are the actions management establishes through

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

Fraud Assessment

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

Data Reliability

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

Government Standards

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

Appendix D: VA Management Comments

Department of Veterans Affairs Memorandum

Date: October 30, 2022

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

Subj: OIG Draft Report: Inspection of Information Technology Security at the Southern Oregon Rehabilitation Center and Clinics, Project Number 2022-01836-AE-0080 (VIEWS 08545826)

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

1. The Office of Information and Technology (OIT) is responding to the Office of Inspector General (OIG) draft report, Inspection of Information Technology Security at the Southern Oregon Rehabilitation Center and Clinics (Project Number 2022-01836-AE-0080).

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

The OIG removed point of contact information prior to publication.

(Original signed by)

Kurt D. DelBene

Attachment

Attachment

Office of Information and Technology
Comments on Office of Inspector General Draft Report,
Inspection of Information Technology Security at the Southern Oregon *Rehabilitation Center and Clinics,* Project Number 2022-01836-AE-0080
(VIEWS 08545826)

Recommendation 1: Implement a vulnerability management program that ensures system changes within established deadlines.

Comments: Concur.

The Department of Veterans Affairs (VA) Office of Information and Technology (OIT) concurs. VA's overall patch and vulnerability compliance percentages provide evidence that VA has implemented, and is managing, an effective vulnerability management and flaw remediation program, aligned with industry standards. VA consistently maintains a 90% or greater management rate for critical vulnerabilities across the enterprise. VA's latest analysis of OIG's scan results for the Southern Oregon Rehabilitation Center and Clinics displays 99.88% policy compliance. VA will follow-up on remaining pending or status update vulnerability items to ensure those vulnerabilities are addressed to a compliant state.

Expected Completion Date: January 31, 2023.

Recommendation 2: Develop and approve a system security plan and an authorization to operate for the special-purpose system.

Comments: Concur.

VA is developing a system security plan and completing an authority to operate for the special-purpose system.

Expected Completion Date: September 30, 2023.

Recommendation 3: Include language for contractors to follow federal and VA information technology security requirements in contracts that have an information technology component.

Comments: Concur.

VA submitted a contract modification to ensure the relevant Federal Acquisition Regulation clause is included in contracts that have an information technology component.

Expected Completion Date: January 31, 2023.

Recommendation 4: Verify that access control lists have been applied to network segments that contain medical systems.

Comments: Non-concur.

Southern Oregon Rehabilitation Center and Clinics disagrees that the network segments OIG identified contain sensitive devices requiring isolation using access control lists. The devices identified by OIG do not meet the definition of devices requiring isolation as defined by VA's Office of Information Security.

Expected Completion Date: Completed.

VA OIT requests removal or closure of Recommendation 4.

Recommendation 5: Develop and implement a process to retain database logs for a period consistent with VA's record retention policy.

Comments: Concur.

VA concurs with the finding that devices identified by OIG did not retain database logs for a period consistent with VA's record retention policy. VA has corrected the issue, as detailed in the supporting evidence.

Expected Completion Date: Completed.

VA requests removal or closure of Recommendation 5.

Recommendation 6: Develop and implement controls to remove an individual's access rights to computer rooms when access is no longer necessary.

Comments: Concur.

Southern Oregon Rehabilitation Center and Clinics Management Services implemented a visitor log to track and control access to computer rooms.

Expected Completion Date: Completed.

VA requests removal or closure of Recommendation 6.

Recommendation 7: Implement a process to regularly review applicable reports to ensure that only authorized individuals have computer room access and update the system access authorization memo to include only those individuals necessary to perform job functions.

Comments: Concur.

Southern Oregon Rehabilitation Center and Clinics will modify access to the OIT-controlled access areas to include quarterly reviews of applicable reports to ensure only individuals included in the standard operating procedure have access to all controlled areas. A new access list was signed and distributed. The physical access control systems manager modified physical access to reflect the new access list. Facility Management Services implemented required physical security measures to control access to the sensitive areas identified by OIG. Additionally, VA Police Department will now inspect newly implemented physical security controls on a routine basis. All changes were completed on or before July 28, 2022.

Expected Completion Date: Completed.

VA requests removal or closure of Recommendation 7.

Recommendation 8: Validate that appropriate physical and environmental security measures are implemented and functioning as intended.

Comments: Concur.

Southern Oregon Rehabilitation Center and Clinics initiated work orders to ensure that all appropriate physical and environmental security measures are implemented and functioning properly.

Expected Completion Date: December 31, 2024.

Recommendation 9: Inventory and verify that records containing personally identifiable information and personal health information are adequately secured.

Comments: Concur.

The unsecured records identified by OIG were reported and the records secured in accordance with VA and Veterans Health Administration incident response procedures. The incident ticket was closed upon completion of the incident management process.

Expected Completion Date: Completed.

VA OIT requests removal or closure of Recommendation 9.

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

OIG Contact and Staff Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Inspection Team	Michael Bowman, Director Luis Alicea Keith Hargrove Shawn Hill Timothy Moorehead Albert Schmidt
Other Contributors	Charles Hoskinson

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, VISN 20: VA Northwest Health Network
Director, Southern Oregon Rehabilitation Center and Clinics

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
U.S. Senate: Jeff Merkley, Ron Wyden
U.S. House of Representatives: Cliff Bentz

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