US DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS HEALTH ADMINISTRATION

Follow-Up Inspection of Information Security at the VA Southern Oregon Healthcare System

Information Security Inspection	25-02402-83	June 25, 2026

OUR MISSION

To conduct independent oversight of the Department of Veterans Affairs that combats fraud, waste, and abuse and improves the effectiveness and efficiency of programs and operations that provide for the health and welfare of veterans, their families, caregivers, and survivors.

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

The VA Office of Inspector General (OIG) conducted a follow-up inspection of the Southern Oregon Healthcare System to assess compliance with federal cybersecurity standards under the Federal Information Security Modernization Act of 2014 (FISMA).[1] This system was previously inspected in 2022 and was selected for follow-up due to prior findings and because it has since implemented the federal Electronic Health Record (EHR) system.[2] For the current inspection, the OIG visited the Southern Oregon Healthcare System during May 2025. The OIG team focused on three security control categories: configuration management, security management, and access controls.

In August 2025, the OIG provided VA with details of its preliminary findings and recommendations, which VA initiated actions to address. The communication of preliminary findings and recommendations to VA contained "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, that internal material is not being published by the OIG or distributed outside VA.

In this follow-up report, the OIG made eight recommendations, including strengthening configuration management and improving network and physical security; four recommendations are similar to recommendations from the 2022 inspection.[3] These repeat deficiencies could compromise the protection of VA data and information systems from unauthorized access, alteration, or destruction. As of February 2026, VA's Office of Information and Technology (OIT) provided sufficient evidence that they fully addressed three of the eight recommendations related to findings concerning access to accounts, physical key management, and the destruction of temporary paper records. Accordingly, recommendations 3, 4, and 8 are considered closed.

In April 2026, the Deputy Secretary of VA, performing the delegable duties of the assistant secretary for OIT and chief information officer, formally responded that VA concurred with all eight recommendations and requested closure of recommendations 1 and 2 based on actions taken. For recommendation 1, while actions were taken to provide agency oversight into the vulnerabilities on the network, there are still some vulnerabilities that require plans of action and milestones. For recommendation 2, VA provided documentation supporting that a network device had been updated to meet secure baseline configurations; however, further supporting

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

[2] VA OIG, *Inspection of Information Security at the Southern Oregon Rehabilitation Center and Clinics*, Report No. 22-01836-12, January 18, 2023.

[3] The full list of recommendations can be found in the report along with VA's response and action plan, which is available in appendix C.

documentation is needed regarding other updates. Finally, OIT provided corrective action plans for recommendations 5 through 7. The full response is available in appendix C.

What the Inspection Found

The OIG identified two serious configuration management deficiencies at the VA Southern Oregon Healthcare System that left its network vulnerable. First, staff at the system missed VA's deadline to fix critical vulnerabilities and did not create required action plans—leaving the network exposed to potential unauthorized access or operational disruption. Second, selected infrastructure components were not fully aligned with approved security baselines. These weaknesses in vulnerability tracking and system configuration put veterans' data and VA's healthcare operations at serious risk of unauthorized access or operational disruption.

The OIG found two security issues at the Southern Oregon system that put veterans' personal data at risk. First, staff did not promptly disable system access for some temporary staff who left their position early. Second, some VA users, including volunteers and clerks, had broad access to information in the EHR system. These issues increase the risk of data breaches and reputational harm.

The OIG identified five critical access control deficiencies at the White City VA Medical Center—part of the Southern Oregon Healthcare System—that put veterans' care and data at serious risk. First, separation of duties and inventory controls for physical keys require strengthening to ensure effective physical access governance. Second, network infrastructure was open to tampering. Third, environmental control compliance—including equipment grounding—requires improvement in selected locations. Fourth, certain network distribution areas require enhanced continuity controls to maintain availability during power events. Last, records destruction oversight controls require enforcement to ensure a designated witness observes destruction activities. These issues are threats to operations, data integrity, and VA's reputation.

Next Steps

The OIG will continue to evaluate VA OIT's actions and will close the remaining open recommendations once the office provides complete documentation and sufficient evidence that it has addressed the intent of the recommendations and the issues identified in this report.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

Contents

Abbreviations

EHR	Electronic Health Record
FISCAM	*Federal Information System Controls Audit Manual*
FISMA	Federal Information Security Modernization Act of 2014
GAO	Government Accountability Office
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, and destruction.[4] 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.[5] The FISMA audit is conducted in accordance with guidelines issued by the Office of Management and Budget and the National Institute of Standards and Technology (NIST).[6]

The OIG conducts information security inspections that provide specific recommendations to VA on enhancing information security oversight at local and regional facilities. Appendix A presents information about FISMA and other federal criteria and standards discussed in this report. Typically, facilities selected for these inspections either were not included in the annual FISMA audit or had previously performed poorly. This system was inspected in 2022 and was selected for follow-up due to prior issues and because it has since implemented the federal Electronic Health Record (EHR) system.[7]

The OIG's prior inspection of the VA Southern Oregon Healthcare System made nine recommendations to correct identified security weaknesses.[8] This follow-up inspection was conducted to determine whether the healthcare system's information security systems were meeting federal security guidance as related to configuration management, security management, and access controls.[9] Furthermore, this inspection sought to determine whether VA had taken appropriate corrective actions. The inspection team visited the White City VA Medical Center—part of the Southern Oregon Healthcare System—in May 2025. The team found that VA's Office of Information and Technology (OIT) made progress in addressing the recommendations from the 2022 OIG inspection, but issues remained.

The OIG provided VA with details of its preliminary findings and recommendations in August 2025. The communication included conditions that contained "VA Sensitive Data" as defined in 38 U.S.C. § 5727. Federal law, including FISMA and its implementing regulations,

---

[4] Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016; US Department of Commerce, National Institute of Standards and Technology (NIST), Joint Task Force, NIST Special Publication 800-53 revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, September 2020, updated December 10, 2020.

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

[6] OMB Circular A-130; NIST Special Publication 800-53 revision 5.

[7] VA OIG, *Inspection of Information Security at the Southern Oregon Rehabilitation Center and Clinics*, Report No 22-01836-12, January 18, 2023.

[8] VA OIG, *Inspection of Information Security at the Southern Oregon Rehabilitation Center and Clinics.*

[9] The scope and methodology of this follow-up inspection are detailed in appendix B.

requires federal agencies to protect sensitive data and information systems due to the risk of harm that could result from improper disclosure. Accordingly, that material is not being published by the OIG or distributed outside VA.

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

Security Controls

Both the Office of Management and Budget and NIST provide criteria for implementing security controls.[10] NIST establishes security and privacy controls for systems and organizations so organizations can identify the controls needed to manage risk and to satisfy federal security and privacy requirements.[11] According to the Office of Management and Budget, security and privacy control assessments ensure that controls selected by agencies are implemented correctly, operate as intended, and effectively satisfy security and privacy requirements.[12]

The assistant secretary for information and technology, who is also VA's chief information officer, oversees the risk management framework for VA information systems and the VA information security program and directs and oversees the cybersecurity risk management of VA information technology.[13] VA has a risk-based process for selecting system security controls. VA's risk management framework aligns security controls and assessment procedures with NIST and provides guidance to help information system owners select the appropriate controls to secure their systems.[14]

This OIG information security inspection focused on three selected security control areas from the *Federal Information System Controls Audit Manual* (*FISCAM*) as shown in table 1. *FISCAM* groups related NIST security and privacy controls into categories that have similar types of risks.[15]

[10] OMB, "Security of Federal Automated Information Resources," app. III in OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016; NIST Special Publication 800-53 revision 5.

[11] NIST Special Publication 800-53 revision 5.

[12] OMB Circular A-130.

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

[14] VA Handbook 6500.

[15] Government Accountability Office (GAO), *Federal Information System Controls Audit Manual (FISCAM)*, GAO-24-107026, September 2024.

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.	Baseline configurations, configuration settings, vulnerability management, and flaw remediation
Security management	Establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security controls, and monitoring the effectiveness of the controls.	Risk management, assessment, authorization, and monitoring
Access	Limit access and detect inappropriate access to information resources.	Access, identification, authentication, and accountability, including related physical security controls

Source: VA OIG analysis of FISCAM.

Without these critical controls, VA's systems would be at risk of unauthorized access that could compromise their confidentiality, integrity, and availability. Furthermore, a cyberattack could disrupt access to, destroy, or allow malicious control of personal information belonging to VA patients, dependents, beneficiaries, employees, contractors, or volunteers.

Office of Information and Technology Structure and Responsibilities

The assistant secretary for information and technology serves as chief information officer and leads OIT.[16] OIT's end user operations team provides on-site support to information technology customers across all VA administrations and program offices—including VA employees and contractors with government-furnished information technology equipment.[17] End user operations staff assigned to the VA Southern Oregon Healthcare System are responsible for managing system plans of action and milestones to ensure all assessed and scanned vulnerabilities are documented.[18] The Cybersecurity Operations Center, part of the Office of Information Security, serves as the authoritative source for addressing and managing cybersecurity incidents.[19]

Results of Previous Reports

Prior OIG and Government Accountability Office (GAO) VA-wide audits have previously reported recurring information security challenges, particularly regarding configuration

[16] VA Handbook 6500; VA, *VA Functional Organization Manual, Volume 2 of 2: Staff Offices*, ver. 8.1, 2023.

[17] VA, *VA Functional Organization Manual*.

[18] VA OIT, End User Services (EUS), *End User Operations (EUO), Security Controls - Risk Assessment (RA) Standard Operating Procedure (SOP)*, ver. 1.0.3, March 18, 2025.

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

management, security management, and access controls.[20] These deficiencies could compromise the protection of VA data and information systems.

VA Southern Oregon Healthcare System

The VA Southern Oregon Healthcare System consists of the White City VA Medical Center and the Grants Pass and Klamath Falls community-based outpatient clinics. In fiscal year 2024, the medical center provided care to over 14,000 patients. According to OIT documentation, the medical center had nearly 900 employees and a budget of more than $309 million for fiscal year 2025.

[20] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2024*, Report No. 24-01233-90, June 18, 2025; GAO, *Cybersecurity: VA Needs to Address Privacy and Security Challenges*, GAO-23-106412, April 18, 2023; GAO, *Chief Information Officer Open Recommendations: Department of Veterans Affairs*, GAO-26-108706, January 22, 2026.

Results and Recommendations

The inspection team reviewed configuration management, security management, and access controls at the Southern Oregon Healthcare System, areas determined to be of the highest risk of not adequately protecting veterans' sensitive data based on the OIG's previous inspection. Although the Southern Oregon Healthcare System had improved, the team identified persistent deficiencies related to all three areas assessed. Table 2 summarizes the findings and recommendations from the previous inspection and shows whether facility managers implemented effective controls to address prior recommendations or if the problems persisted, resulting in repeat findings in fiscal year 2025.[21]

Table 2. Evaluation of Actions Addressing Prior Recommendations for the Southern Oregon Healthcare System

Control area	Prior finding	Prior recommendation	Repeat finding in fiscal year 2025
Configuration management	Hosts on the healthcare system's network used unsupported versions of applications and had missing patches.	Implement a vulnerability management program that ensures system changes within established deadlines.	Yes
Security management	The healthcare system's special-purpose system lacked authorization to operate.	Develop and approve a system security plan and an authorization to operate for the special-purpose system. Include language for contractors to follow federal and VA information technology security requirements in contracts that have an information technology component.	No
Access	Network segmentation controls were missing for multiple network segments that contained medical systems.	Verify that access control lists have been applied to network segments that contain medical systems.	No

[21] VA OIG, *Inspection of Information Security at the Southern Oregon Rehabilitation Center and Clinics.*

Control area	Prior finding	Prior recommendation	Repeat finding in fiscal year 2025
Access	Physical access to computer rooms, communication closets, and generators was not adequately restricted.	Develop and implement controls to remove an individual's access rights to computer rooms when access is no longer necessary. 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.	Yes
Access	Environmental controls were not fully implemented in certain computer rooms and communications closets, including grounding electrical equipment, monitoring of temperature and humidity, and using fire detection and suppression systems.	Validate that appropriate physical and environmental security measures are implemented and functioning as intended.	Yes
Access	Database managers did not adequately maintain log data for local databases.	Develop and implement a process to retain database logs for a period consistent with VA's records retention policy.	No
Access	Federal records were not properly managed and safeguarded throughout their life cycles.	Inventory and verify that records containing personally identifiable information and personal health information are adequately secured.	No

Source: VA OIG analysis of the prior report findings and follow-up inspection results.

While the VA Southern Oregon Healthcare System has improved its configuration management processes to address some deficiencies, the inspection team identified repeat security weaknesses related to vulnerability remediation processes designed to protect sensitive information. During the review of security management controls, the team determined that VA established the needed authorization to operate for a national special-purpose system, which includes the special-purpose systems at the Southern Oregon Healthcare System. Separately, the team identified a deficiency with user account management. Finally, the team determined that the

contract for a special-purpose system did include language requiring the contractor to adhere to federal and VA security requirements. The team also identified deficiencies in physical access controls.

I. Configuration Management

According to GAO's *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 operation.[22] An effective configuration management process should be described in a configuration management plan and then implemented according to that plan.

To evaluate this control area, the team interviewed OIT staff. The inspection team also examined whether the Southern Oregon Healthcare System identified and remediated vulnerabilities within established time frames and configured its servers according to standards.

Finding 1: The Healthcare System Had Two Configuration Management Deficiencies

The inspection team concluded that the healthcare system had two deficiencies in configuration management controls. Analysis of OIT's vulnerability scan results and its plans of action and milestones showed the facility did not create plans of action and milestones for vulnerabilities persisting past the limit set by VA.[23] The team also found that some systems on the healthcare system's network were running software that was not configured according to approved security baselines.

Vulnerability Remediation

FISMA audits have repeatedly identified deficiencies in VA's vulnerability management controls. Consistent with those findings, the team identified deficient controls at the VA Southern Oregon Healthcare System.

Vulnerability management is how an organization identifies, classifies, and reduces weaknesses. It also helps organizations assess risks and monitor the effectiveness of its overall security program. At VA, OIT conducts routine and random vulnerability scans and reports the identified vulnerabilities to facilities for remediation. In 2023, OIT implemented a formal process to track the monitoring and remediation of vulnerabilities by using a plan of action and milestones. The new tracking process makes information system stewards responsible for entering all critical- and high-severity vulnerabilities that cannot be remediated timely into a plan of action and

[22] Firmware refers to computer programs and data stored in hardware, typically in read-only memory, that cannot be written or changed during the execution of the program. GAO, *FISCAM*.

[23] VA Information Security Knowledge Service, "Security Controls Explorer," April 9, 2024.

milestones for remediation.[24] Information system stewards should document the actions taken to correct deficiencies.[25]

NIST guidance calls for a severity level to be assigned to each vulnerability using the Common Vulnerability Scoring System.[26] The inspection team's testing of vulnerability remediation focused on whether critical and high vulnerabilities were remediated within agency-approved timelines. Both the OIT-provided network vulnerability scan and the OIG scans showed a high number of vulnerabilities persisting past deadlines. The OIG provided VA OIT the details of the vulnerabilities and associated hosts that required remediation, including vulnerabilities not identified in VA's vulnerability reports.[27]

System Baseline Configuration

During the inspection, the team also scanned the configurable settings on selected infrastructure components at the healthcare systems to check compliance with secure baselines. According to VA policy, these servers should be securely configured as part of the standard system development process, and systems should be configured using baselines that have been documented, formally reviewed, and agreed upon by managers.[28] Despite VA policy, certain software configuration settings did not meet baseline security requirements.

Specifically, the inspection team identified category 1 security configuration issues on a network device. An exploitation of category 1 configuration vulnerability "will directly and immediately result in loss of confidentiality, availability, or integrity."[29] The team also identified security configuration issues on multiple databases. Given the potential severity of such issues, security

[24] The vulnerabilities severity level is based on the Common Vulnerability Scoring System developed by the Forum of Incident Response and Security Teams and is a standardized framework used to evaluate the severity of software vulnerabilities. It provides a numerical score ranging from low, moderate, high, and critical based on various factors including attack complexity, the ability to perform attack remotely, privileges required, effect of the attack, and the availability and sophistication of exploit tools.

[25] According to the NIST Computer Security Resource Center Glossary, an information system steward is an "agency official with statutory or operational authority for specified information and responsibility for establishing controls for its generation, collection, processing, dissemination, and disposal." "Glossary" (web page), NIST Computer Security Resource Center, accessed May 14, 2025, https://csrc.nist.gov/glossary/term/information_steward.

[26] "Vulnerability Metrics" (web page), NIST National Vulnerability Database, accessed August 11, 2025, https://nvd.nist.gov/vuln-metrics/cvss; "Common Vulnerability Scoring System version. 4.0, Specification Document, Revision 2," Forum of Incident Response and Security Teams, accessed February 2, 2026, https://www.first.org/cvss/v4-0/cvss-v40-specification.pdf.

[27] According to the NIST Computer Security Resource Center Glossary, "a host is any hardware device that has the capability of permitting access to a network via a user interface, specialized software, network address, protocol stack, or any other means." "Glossary" (web page), NIST Computer Security Resource Center, accessed May 14, 2025, https://csrc.nist.gov/glossary/term/host.

[28] VA Handbook 6500.

[29] Defense Information Systems Agency, *Application Security and Development Security Technical Implementation Guide Overview*, ver. 6, rev. 3, April 2, 2025.

configuration of servers is not only a defensive strategy but also a proactive one that helps protect VA systems.

During the inspection, OIT provided evidence that they had remediated the baseline issues related to a network device, while other remediation efforts were ongoing.

Finding 1 Conclusion

Numerous system vulnerabilities were not mitigated on time, and software did not meet baseline requirements, leaving the VA Southern Oregon Healthcare System's network and veteran's data exposed to potential unauthorized access or operational disruption.

Recommendations 1–2

The OIG made the following recommendations to the assistant secretary for information and technology and chief information officer:[30]

1. Improve the existing vulnerability management process to make sure all vulnerabilities are identified, plans of action and milestones are created for vulnerabilities that cannot be mitigated by VA deadlines, and software is updated before vendor support ends.
2. Implement a baseline configuration process to make sure network devices and databases are running authorized software that is configured to approved baselines and free of vulnerabilities.

VA Management Comments

In April 2026, the Deputy Secretary of VA, performing the delegable duties of the acting assistant secretary for information and technology and chief information officer, concurred with recommendations 1 and 2. For recommendation 1, he stated that OIT addressed the vulnerability management issues at the facility, and has either remediated the vulnerabilities or formally documented plans of action and milestones. As a result, VA requested that recommendation 1 be closed.

In response to recommendation 2, the Deputy Secretary indicated OIT implemented a baseline configuration process for network devices and databases, upgraded software, resolved noncompliant configurations, and completed connectivity testing. As a result, VA requested that recommendation 2 be closed. The full text of the Deputy Secretary's response is included in appendix C.

[30] The recommendations addressed to the assistant secretary for information and technology and chief information officer are directed to anyone in an acting status or performing the delegable duties of the position.

OIG Response

For recommendation 1, while actions were taken to provide agency oversight into the vulnerabilities on the network, according to OIT's reports, there are still some vulnerabilities that require plans of action and milestones. For recommendation 2, VA provided documentation supporting that a network device had been updated to meet secure baseline configurations; however, further supporting documentation is needed regarding other updates. The OIG will monitor implementation of the planned actions and will close recommendations 1 and 2 when VA provides evidence demonstrating they have addressed the identified issues.

II. Security Management Controls

According to *FISCAM*, security management controls establish a framework and a continuous cycle for assessing risk, developing security procedures, and monitoring the effectiveness of the procedures. The inspection team evaluated EHR user and account management controls at the Southern Oregon Healthcare System. To assess these controls, the inspection team reviewed standard operating procedures and applicable VA policies. These included documentation from VA's cybersecurity management service for workflow automation and continuous monitoring. The team interviewed system security officers, biomedical staff, and the area manager. The team also conducted a walk-through of the White City medical center.

Finding 2: The Healthcare System Had Two Security Management Deficiencies

The inspection team concluded that the healthcare system had two deficiencies in security management controls. The healthcare system did not promptly disable EHR and network access for temporary staff who left early, resulting in accounts remaining active after the staff's departure. The OIG also found that some VA users had unnecessary access to a screen with personally identifiable information in the EHR system.

Access to Accounts

The OIG determined that the healthcare system did not have a process to promptly remove access to EHR and network accounts for temporary staff who left their position early. To access EHR, users need to have a VA network and EHR account. The network accounts are set to be disabled for temporary staff at the expected end date of their agreement. The OIG identified that EHR and network accounts remained enabled for a duration of time for certain temporary staff who left earlier than expected. The inspection team determined that the accounts had not been used after the staff left their position. Regardless, the facility should implement a process to disable network and EHR access for temporary staff who left early. An individual who retains access after separation could obtain information for unauthorized disclosure or modify information in the system that could affect operations.

During the inspection, OIT provided support that they updated account management to include processes to disable access to the active directory and the EHR when temporary staff leave before their expected end date.

Security of Personally Identifiable Information

The OIG discovered that some VA users (including volunteers and scheduling clerks) with access to the federal EHR had broad access to a screen that included personally identifiable information not needed based on job responsibility. The OIG initially observed this access during

an earlier information security inspection.[31] In that report, the OIG recommended a cost-benefit analysis with appropriate controls being implemented in EHR to limit disclosure of veterans' personally identifiable information based on job responsibility. In response, VA said that all VA users, including scheduling clerks and volunteers, must complete annual security and privacy training courses appropriate to their roles before being granted access to systems. VA stated that the federal EHR uses predefined, standardized, curated user roles, and that the practice follows the "need to know" principle and is compliant with Veterans Health Administration (VHA) Directive 1605.02.[32] VA concurred with the recommendation and plans to conduct an impact analysis of user role access within the federal EHR system. VA's action plans, once implemented, should address the issue for all facilities hosting the federal EHR.

Finding 2 Conclusion

The healthcare system lacked a process to promptly disable EHR and network access of temporary staff who left early, and had users with unnecessary access to a screen with personally identifiable information in the EHR system. A breach of personally identifiable information could result in a financial and reputational loss to VA, which is entrusted to protect sensitive veteran data.

Recommendation 3

The OIG made the following recommendation to the assistant secretary for information and technology and chief information officer, in coordination with the White City VA Medical Center director:[33]

3. Implement a process to disable access to the active directory and the electronic health record when temporary staff leave before their expected end date.

In response to the OIG's inspection findings, VA provided documentation of corrective actions in February 2026, and the OIG considers recommendation 3 closed. The Deputy Secretary, performing the delegable duties of the acting assistant secretary for information and technology and chief information officer, concurred with the recommendation in VA's response, which is in appendix C.

[31] VA OIG, *Inspection of Information Security at the Spokane Healthcare System in Washington*, Report No. 25-00975-234, February 18, 2026.

[32] VHA Directive 1605.02, *Minimum Necessary Standard for Access, Use, Disclosure, and Requests for Protected Health Information*, April 4, 2019.

[33] The recommendations addressed to the assistant secretary for information and technology and chief information officer are directed to anyone in an acting status or performing the delegable duties of the position.

III. Access Controls

According to *FISCAM*, access controls limit access or detect inappropriate access to information resources, and protect these resources against unauthorized modification, loss, and disclosure. Access controls address logical and physical access. Logical access controls include user authentication, access to resources, and user permissions for actions. Physical access controls restrict physical access to information resources and facilities.[34] Annual FISMA reports have repeatedly identified access controls as a nationwide issue for VA.[35] To evaluate the White City VA Medical Center access controls, the inspection team interviewed OIT and facility staff, reviewed local policies and procedures, and conducted walk-throughs of the facility.[36] The inspection team reviewed access and environmental controls over the computer room and communications closets at the White City VA Medical Center.[37]

Finding 3: The Healthcare System Had Five Access Control Deficiencies

The OIG identified issues with the management of keys, unsecured network infrastructure, electrical grounding, uninterruptible power supplies, and the destruction of temporary records.

Management of Physical Keys

The inspection team discovered that physical access to the facility and its information technology resources was not effectively controlled. While the facility had a process for assigning physical keys, the blank key stock was maintained by the same individuals who could make keys. As a result, these individuals had the ability to make unauthorized keys. Furthermore, there was no inventory of blank key stock to be able to determine whether unauthorized keys were made.

During the inspection, OIT provided evidence that they separated the duties of maintaining physical blank key stock and making keys to improve physical access controls over key inventories.

Unsecured Infrastructure

Network infrastructure at the facility was not properly secured. Specifically, the inspection team found that exposed network infrastructure did not meet VA environmental security

[34] GAO, *FISCAM*.

[35] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2024*.

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

[37] *FISCAM* critical elements for access controls are listed in appendix A.

requirements.[38] Damage to the infrastructure could negatively affect the facility's ability to provide healthcare services to veterans.

Electrical Grounding

An information technology area and some other spaces at the medical center did not meet federal and VA environmental security requirements related to grounding of equipment.[39] The center's staff were unaware the equipment was not properly grounded. Without proper grounding, equipment could be damaged by energy bursts. Additionally, not having a proper grounding network could reduce the ability for the facility to provide health care, negatively affecting patient health.

Uninterruptible Power Supply

During a tour of the facility, the inspection team determined that certain locations lacked appropriate emergency power coverage. Not having adequate uninterruptible power supply coverage could have a negative effect on the facility's ability to provide health care.

Monitoring of Temporary Records Destruction

The healthcare system did not have a process for a witness to observe a contractor's on-site destruction of temporary paper records that contained personally identifiable information.[40] Federal and VA requirements state that a witness must observe the destruction of such documents; however, no witness observed the destruction of these documents at the medical center.[41] As a result, the healthcare system had no assurance that the paper records were appropriately destroyed. VA is entrusted to protect sensitive veteran data, and a compromise of these temporary paper records could result in a financial and reputational loss.

During the inspection, OIT provided evidence that they established a process to make sure a witness observes the destruction of temporary paper files that contain personally identifiable information and protected health information.

---

[38] *VA Physical Security and Resiliency Design Manual,* October 1, 2020, revised May 1, 2024.

[39] NIST Special Publication 800-53 revision 5; VA, *Infrastructure Standard for Telecommunications Spaces*, version 3.1, July 1, 2021.

[40] According to VA Directive 6371, *Destruction of Temporary Paper Records*, April 8, 2014, the "destruction carried out by an information destruction contractor must be witnessed by a VA employee or, if authorized by the VA organization that created the temporary paper records, a contractor (or subcontractor or third party) employee may act as witness."

[41] 36 C.F.R. § 1226.24; "Disposition of Federal Records: A Records Management Handbook" (web page), National Archives Administration, accessed November 18, 2024, https://www.archives.gov/files/records-mgmt/pdf/dfr-2000.pdf; VA Directive 6371.

Finding 3 Conclusion

The OIG concluded that the VA Southern Oregon Healthcare System had significant deficiencies in five critical access control areas, which could compromise the security and reliability of its information technology infrastructure. Weaknesses in key management allowed individuals to potentially create unauthorized keys due to a lack of separation of duty controls. Additionally, many server rooms and other areas were not properly grounded, exposing equipment to potential damage from electrical events. Certain locations also lacked appropriate emergency power coverage, threatening continuity of care during power outages. Finally, the facility did not ensure proper oversight of temporary records destruction, leaving sensitive veteran information vulnerable to unauthorized disclosure.

Recommendations 4–8

The OIG made the following recommendations to the assistant secretary for information and technology and chief information officer, in coordination with the White City VA Medical Center director:[42]

4. Separate the duties of maintaining physical blank key stock and making keys to improve physical access controls over key inventories.
5. Secure network infrastructure in accordance with VA environmental protection standards.
6. Complete the installation of grounding measures for all telecommunication closets to protect information technology equipment.
7. Routinely monitor and service uninterruptible power supplies that support the network infrastructure.
8. Establish a process to make sure a witness observes the destruction of temporary paper files that contain personally identifiable information and protected health information.

Based on the evidence of corrective actions provided by VA in February 2026, the OIG considers recommendations 4 and 8 closed.

VA Management Comments

The Deputy Secretary of VA, performing the delegable duties of the assistant secretary for information and technology and chief information officer, concurred with recommendations 4 through 8. In response to recommendation 5, he stated the facility will secure all exposed

[42] The recommendations addressed to the assistant secretary for information and technology and chief information officer are directed to anyone in an acting status or performing the delegable duties of the position.

cables by installing protective conduits and will lock associated manhole covers. For recommendation 6, the Deputy Secretary indicated the facility will install grounding measures. Finally, to address recommendation 7, he stated the facility will implement monitoring controls for the uninterruptible power supplies and noted the facility replaced those uninterruptible power supply units that were identified with operational devices. The full text of the Deputy Secretary's response is included in appendix C.

OIG Response

The corrective action plans are responsive to the intent of the recommendations. The OIG will monitor implementation of the remaining planned actions and will close recommendations 5, 6, and 7 when VA provides evidence demonstrating they have addressed the identified issues.

Appendix A: Additional Background

Federal Information Security Modernization Act of 2014 (FISMA)

The following are the stated goals of FISMA:

- 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 the development and maintenance of the 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.

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 VA Office of Inspector General (OIG) accomplishes the annual FISMA evaluation through a contracted external auditor and oversees the contractor's performance.

National Institute of Standards and Technology Information Security Guidelines

The National Institute of Standards and Technology (NIST) is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems.[43] NIST develops information security standards and guidelines in

[43] US Department of Commerce, National Institute of Standards and Technology (NIST), Joint Task Force, NIST Special Publication 800-53 revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020, updated December 10, 2020.

accordance with its statutory responsibilities under FISMA. NIST Special Publication 800-53 provides a catalog of security and privacy controls for information systems and organizations.[44]

Federal Information System Controls Audit Manual (FISCAM)

The Government Accountability Office developed *FISCAM*, a methodology for evaluating the confidentiality, integrity, and availability of information systems. *FISCAM* groups information categories of similar risks into the following six broad categories: business process controls, security management, access controls, configuration management, separation of duties, and contingency planning.[45] *FISCAM* aligns control categories with NIST controls to help auditors evaluate information systems.

[44] NIST Special Publication 800-53 revision 5.

[45] Government Accountability Office (GAO), *Federal Information System Controls Audit Manual (FISCAM)*, GAO-24-107026, September 2024.

Appendix B: Scope and Methodology

Scope

The inspection team conducted its work from April 2025 through February 2026. The team evaluated configuration management, security management, and access controls of operational VA information security assets and resources in accordance with the Federal Information Security Modernization Act of 2014 (FISMA), National Institute of Standards and Technology (NIST) security guidelines, and VA's information security policy. In addition, the team assessed the capabilities and effectiveness of information 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 and inspected the VA Southern Oregon Healthcare System and its information systems for security compliance. Additionally, the team interviewed VA staff responsible for the facility's information technology security and operations. Furthermore, the team conducted an on-site physical security review of the White City VA Medical Center. To determine local systems' security compliance, the team conducted vulnerability and configuration testing for the VA Southern Oregon Healthcare System at the White City facility. Finally, the team analyzed the results of testing, interviews, and the inspection to identify policy violations and threats to security.

Internal Controls

Using the Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government*, the OIG team assessed internal controls to determine whether they were significant to the inspection objective.[46] This included consideration of the five internal control components: control environment, risk assessment, control activities, information and communication, and monitoring. The team identified one component and one principle as significant to the objective: Component—Control Activities, and Principle 11—"Management should design general control activities over information technology to mitigate risks to achieving the entity's objectives to acceptable levels."[47] The inspection team identified internal control weaknesses during the inspection and proposed recommendations to address them.

[46] Government Accountability Office (GAO), *Standards for Internal Control in the Federal Government*, GAO-25-107721, May 15, 2025.

[47] Since the review was limited to the internal control components and underlying principles identified, it may not have disclosed all internal control deficiencies that may have existed at the time of this review.

Data Reliability

The inspection team generated computer-processed data by using network scanning tools. The results of the scans were provided to OIT. In this process, the team was not testing VA data or systems for transactional accuracy. The security tools identified versions of software hosted on systems to determine whether there were any vulnerabilities associated with the software tested. The tool would identify software versions that have vulnerabilities and would also identify unsupported software. The team relied on the results of the scanning tool and network device configuration. The team performed its own scans to determine whether the agency scans were complete and accurate, met intended purposes, and were not subject to alteration. The team did not find any material differences between OIG and agency scan data and determined the data used were complete and accurate.

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*.[48]

[48] Council of the Inspectors General on Integrity and Efficiency, *Quality Standards for Inspection and Evaluation*, December 2020.

Appendix C: VA Management Comments

Department of Veterans Affairs Memorandum

Date: March 26, 2026

From: Deputy Secretary of Veterans Affairs, Performing the Delegable Duties of the Assistant Secretary for Information and Technology and Chief Information Officer (005)

Subj: Office of Inspector General Draft Report, Follow-Up Inspection of Information Security at the VA Southern Oregon Healthcare System, Project Number 2025-02402-AE-0098 (VIEWS 14431703)

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

1.Thank you for the opportunity to review the Office of Inspector General's (OIG) draft report, Follow-Up Inspection of Information Security at the VA Southern Oregon Healthcare System (Project Number 2025-02402-AE-0098).

2.The Office of Information and Technology (OIT) is committed to ensuring appropriate information security controls are in place at Department of Veterans Affairs (VA) facilities to protect VA systems and data in compliance with Federal security guidance.

3.OIG made eight recommendations, of which OIT concurs with all eight. Based on the evidence of corrective actions previously provided by OIT, OIG considers recommendations 3-4 and 8 to be closed. In the written comments, OIT is providing additional evidence showing that OIT has fully addressed recommendations 1-2. Finally, OIT is providing a corrective action plan and target implementation date for the remaining three open recommendations 5-7.

The OIG removed point of contact information prior to publication.

(Original signed by)

Paul R. Lawrence, PhD

Attachments

Attachment

Office of Information and Technology
Comments on Office of Inspector General Draft Report,
Follow-Up Inspection of Information Security at the
VA Southern Oregon Healthcare System
Project Number 2025-02402-AE-0098

Recommendation 1: Improve the existing vulnerability management process to make sure all vulnerabilities are identified, plans of action and milestones are created for vulnerabilities that cannot be mitigated by VA deadlines, and software is updated before vendor support ends.

VA Comment: Concur. The Department of Veterans Affairs (VA) Office of Information and Technology (OIT) concurs with the Office of Inspector General's (OIG) recommendation. OIT has addressed vulnerability management issues at the facility. According to the February 2026 asset vulnerability scan, VA has either remediated all identified vulnerabilities or formally documented them in a plan of action and milestones item.

VA requests closure of the recommendation.

Recommendation 2: Implement a baseline configuration process to make sure network devices and databases are running authorized software that is configured to approved baselines and free of vulnerabilities.

VA Comment: Concur. OIT implemented a baseline configuration process for network devices and databases. For network devices, OIT upgraded the core switch software in February 2026. For the Structured Query Language database, OIT resolved the identified non-compliant configurations following the core switch software upgrade. Connectivity testing is complete for the updated software, facility switches, and operating system components.

VA requests closure of the recommendation.

Recommendation 3: Implement a process to disable access to the active directory and the electronic health record when temporary staff leave before their expected end date (Closed).

VA Comment: Concur. The White City Associate Chief of Staff for Education updated the local account management process to ensure timely deactivation of student accounts. All students are now enrolled in the Light Electronic Action Framework clearing station process. The updated process allows the site to efficiently route account closure information to the Electronic Health Record for the vendor to address corresponding accounts.

Based on the evidence of corrective actions provided by VA in February 2026, OIG considers recommendation 3 closed.

Recommendation 4: Separate the duties of maintaining physical blank key stock and making keys to improve physical access controls over key inventories (Closed).

VA Comment: Concur. The facility separated the duties of maintaining physical blank key stock and making keys. The facility now secures key stock in a locked cabinet located in the locksmith supervisor's office. The locksmith supervisor has control over maintaining, safeguarding, and issuing key stock. VA is developing procedural documentation for the new process.

Based on the evidence of corrective actions provided by VA in February 2026, OIG considers recommendation 4 closed.

Recommendation 5: Secure network infrastructure in accordance with VA environmental protection standards.

VA Comment: Concur. To strengthen safety and enhance physical security, Facilities Management Service will secure all exposed cables by installing protective conduits and will lock associated manhole covers.

Recommendation 6: Complete the installation of grounding measures for all telecommunication closets to protect information technology equipment.

VA Comment: Concur. To safeguard information technology equipment, Facilities Management Service will complete the installation of grounding measures in the 14 identified telecommunications closets.

Recommendation 7: Routinely monitor and service uninterruptible power supplies that support the network infrastructure.

VA Comment: Concur. Facilities Management Service will implement monitoring controls for the uninterruptible power supplies supporting facility information technology operations. The facility replaced the three identified uninterruptible power supply units with operational devices. Facilities Management Service staff will continue to monitor all remaining units to ensure reliable power protection.

Recommendation 8: Establish a process to make sure a witness observes the destruction of temporary paper files that contain personally identifiable information and protected health information (Closed).

VA Comment: Concur. The facility established a process through which Facility Management Service provides a VA employee escort to observe the vendor's destruction of temporary paper files containing personally identifiable information and protected health information.

Based on the evidence of corrective actions provided by VA in February 2026, OIG considers recommendation 8 closed.

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	Al Tate, Director Sachin Bagai Nicholas Hartzheim Kimberly Moss Albert Schmidt
Other Contributors	Bill Warhop Rashiya Washington

Report Distribution

VA Distribution

Office of the Secretary
Office of Accountability and Whistleblower Protection
Office of Congressional and Legislative Affairs
Office of General Counsel
Office of Information and Technology
Office of Public and Intergovernmental Affairs
VISN 20: Northwest Network
VA Southern Oregon 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 Government Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget
US Senate: Jeff Merkley, Ron Wyden
US House of Representatives: Cliff Bentz

OIG reports are available at www.vaoig.gov.