US DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS HEALTH ADMINISTRATION

Inspection of Information Security at the VA Spokane Healthcare System in Washington

Information Security Inspection	**25-00975-234**	**February 18, 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

In the VA Office of Inspector General's (OIG) fiscal year (FY) 2024 Federal Information Security Modernization Act (FISMA) audit, 21 of 23 recommendations were repeated from previous years.[1] These repeat deficiencies could compromise the protection of VA data and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

The OIG conducted a site visit to the VA Spokane Healthcare System's Mann-Grandstaff VA Medical Center in Washington from January 29 through February 6, 2025. In April 2025, the OIG provided VA with details of its preliminary findings and recommendations. The communication 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 material is not being published by the OIG or distributed outside VA.

The OIG made seven recommendations to improve configuration management, security management, and access controls to safeguard veterans' information.[2] In December 2025, the Deputy Secretary of VA, performing the delegable duties of the assistant secretary for information and technology and chief information officer, formally responded that VA concurred with all seven recommendations and has initiated action plans. VA requested closure of recommendations 1 and 7. 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 7, VA provided documentation of completed corrective action, and the OIG considers that recommendation closed. The OIG will monitor implementation of the planned actions and will close recommendations 1 through 6 when VA provides evidence demonstrating progress in addressing the identified issues.

What the Inspection Found

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

For configuration management, the OIG concluded that VA staff did not remediate multiple critical and high vulnerabilities within VA-defined time frames and had not developed required action plans. Additionally, some systems were running unsupported software, and several

[1] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2024*, Report No. 24-01233-90, June 18, 2025.

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

devices were not configured according to approved security baselines. These issues increase the risk of unauthorized access and operational disruption.

The OIG identified one security management deficiency involving the protection of personally identifiable information (PII). Volunteers and scheduling clerks had unnecessary access to a screen with unredacted PII in the federal Electronic Health Record (EHR).

The OIG found four access control deficiencies. The facility lacked proper segregation of duties for key distribution; network equipment was not secured in two locations; 11 communications closets lacked proper electrical grounding; and perimeter protection measures for fuel storage did not meet VA guidelines. These weaknesses could result in unauthorized access or damage to critical information technology (IT) infrastructure.

Next Steps

The OIG will continue to evaluate the Office of Information and Technology's actions and will close the 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
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
PII	personally identifiable information

Introduction

Information security controls protect VA systems and data from unauthorized access, use, modification, and 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.[3] 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). Appendix A details the fiscal year (FY) 2024 FISMA audit recommendations.

In 2020, the OIG started an information security inspection program. These inspections provide recommendations to VA on enhancing information security oversight at local and regional facilities. Appendix B 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 sample or had previously performed poorly. Appendix C provides more detail on this inspection's scope and methodology.

The OIG conducted this inspection to determine whether the VA Spokane Healthcare System was meeting federal security guidelines. The OIG selected the VA Spokane Healthcare System because it had not been previously visited as part of the annual FISMA audit. Furthermore, it is one of six healthcare systems using the federal Electronic Health Record (EHR).[4] The OIG has issued multiple oversight reports on VA's rollout of the new EHR system, revealing critical missteps and inadequate controls. VA plans to deploy the system to 13 more sites in 2026.

The inspection team visited the VA Spokane Healthcare System's Mann-Grandstaff VA Medical Center in Washington from January 29 through February 6, 2025. In April 2025, the OIG provided VA with details of its preliminary findings and recommendations. The communication 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 material is not being published by the OIG or distributed outside VA. During 2025, VA worked to address the OIG's preliminary findings and recommendations, and VA filed a formal response to the OIG's recommendations in December 2025.

[3] Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. §§ 3551–3558; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2024*, Report No. 24-01233-90, June 18, 2025.

[4] VA healthcare systems that have implemented the federal EHR so far include the Lovell Federal Healthcare System in Illinois; the Central Ohio Health Care System in Ohio; the Roseburg and VA Southern Oregon Healthcare Systems in Oregon; and the Spokane and Walla Walla Healthcare Systems in Washington.

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

Security Controls

The Office of Management and Budget and NIST provide criteria for implementing security controls.[5] These criteria call for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system.

VA policy outlines NIST and VA requirements to help information system owners choose the appropriate controls to secure their systems.[6] According to VA Directive 6500, responsibility for developing and maintaining information security policies, procedures, and control techniques lies with the assistant secretary for information and technology, who also serves as VA's chief information officer. VA Handbook 6500 describes the risk-based process for selecting system security controls, including operational requirements.

This OIG information security inspection focused on three security control areas 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
Security management	Establish a framework and continuous cycle of activity for managing risk, developing and implementing effective security policies, and monitoring the adequacy of these procedures	Risk management, assessment, authorization, and monitoring

[5] Office of Management and Budget (OMB), "Security of Federal Automated Information Resources," app. 3 in OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016; NIST Special Publication 800-53 revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020.

[6] VA Handbook 6500, *Risk Management Framework for VA Information Systems: VA Information Security Program*, February 2021; VA Directive 6500, *VA Cybersecurity Program*, February 24, 2021. The NIST Computer Security Resource Center's Glossary defines a system owner as a "person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system." "Glossary," NIST Computer Security Resource Center, accessed May 27, 2025, https://csrc.nist.gov/glossary/term/system_owner.

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 of the Federal Information System Controls Audit Manual (FISCAM).[7]

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, who also serves as VA's chief information officer, leads the Office of Information and Technology (OIT). The OIT offices relevant to the areas assessed at the VA Spokane Healthcare System are shown in figure 1.

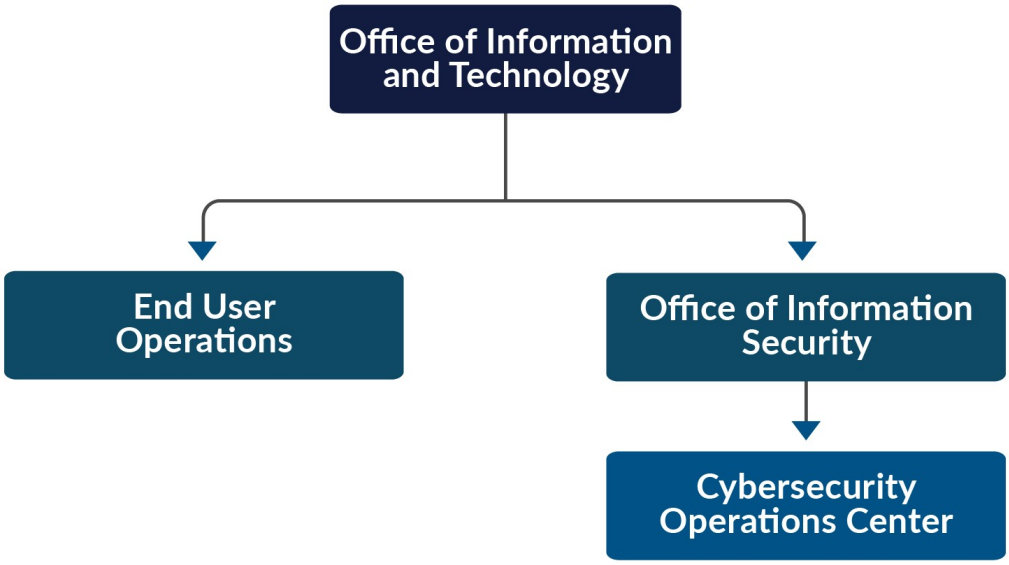

Figure 1. *Organizational structure of OIT entities relevant to this inspection.*
Source: VA OIG analysis.

OIT's End User Operations team provides on-site support to information technology (IT) customers across all VA administrations and program offices—including VA employees and contractors with government-furnished IT equipment and access. End User Operations staff

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

assigned to the VA Spokane Healthcare System are responsible for managing system plans of action and milestones to ensure all assessed and scanned vulnerabilities are documented.[8]

The Cybersecurity Operations Center, which is part of OIT's Office of Information Security, is responsible for protecting VA information and systems by identifying and reporting on emerging and imminent threats and vulnerabilities.

Electronic Health Record Modernization Integration Office

The program executive director of the Electronic Health Record Modernization Integration Office is responsible for implementing the federal EHR. This is part of VA's EHR modernization initiative to store and track patient medical information. As of February 2025, the federal EHR was used at six VA medical centers and 26 VA clinics. VA plans to deploy the federal EHR to 13 more locations in 2026.

Results of Previous Projects

The OIG's FY 2024 FISMA audit was conducted by independent public accounting firm CliftonLarsonAllen LLP. It evaluated 49 major applications and general support systems hosted at 23 VA facilities and tested selected security and privacy controls outlined by NIST.[9] The firm made 23 recommendations, which are listed in appendix A. Of the 23 recommendations, 21 were repeated from the prior annual audit—indicating VA continues to face significant challenges in complying with FISMA requirements.[10] Repeat recommendations included addressing deficiencies in configuration management, security management, and access controls that could compromise the protection of VA data and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

The Government Accountability Office (GAO) has also found that VA has a deficient information security program. GAO reported in 2023 that VA faced several security challenges while securing and modernizing its information systems, including

- fully implementing a process for privacy officials to review IT capital investment plans and budgetary requests;

[8] 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.

[9] The NIST Computer Security Resource Center Glossary defines a general support system as "an interconnected set of information resources under the same direct management control that shares common functionality." "Glossary" (web page), NIST Computer Security Resource Center accessed July 21, 2025, https://csrc.nist.gov/glossary/term/general_support_system.

[10] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2024*. See appendix B for more information.

- establishing clear privacy workforce management procedures, involving the senior agency officials for privacy in hiring, training, and professional development to identify staffing requirements and ensure a qualified workforce;
- fully defining and documenting the role of privacy officials in authorizing information systems with personally identifiable information (PII), as their involvement is not always documented in policies and procedures;
- fully developing a continuous monitoring strategy; and
- providing continual attention to key elements in its cybersecurity risk management strategy, an agencywide risk assessment, identification of enterprise cybersecurity risks, and coordinating between its cybersecurity risk executive and enterprise risk management functions.[11]

VA Spokane Healthcare System

The VA Spokane Healthcare System consists of the Mann-Grandstaff VA Medical Center (shown in figure 2); the Elwood "Bud" Link VA Outpatient Clinic; and the Bonner County, Coeur d'Alene, East Front Avenue, Libby, and Spokane VA clinics.[12] The Mann-Grandstaff VA Medical Center provided care to about 27,000 patients in FY 2024. The facility had over 1,300 employees and a budget of nearly $413 million for FY 2025.

Figure 2. *Mann-Grandstaff VA Medical Center in Spokane, Washington.*
Source: VA OIG, February 5, 2025.

[11] GAO, *Cybersecurity: VA Needs to Address Privacy and Security Challenges*, GAO-23-106412, April 18, 2023.

[12] According to an OIT representative: On April 1, 2025, after the OIG completed fieldwork, the healthcare system opened the Spokane Valley VA Clinic.

Results and Recommendations

I. Configuration Management

According to GAO's *Federal Information System Controls Audit Manual* (*FISCAM)*, configuration management involves identifying and managing security features for all hardware, software, and firmware components of an information system at a given point and systematically controlling changes to that configuration during the system's operation.[13] An effective configuration management process should be described in a configuration management plan and then implemented according to that plan.

OIT's Cybersecurity Operations Center identifies and reports on threats and vulnerabilities in VA. Vulnerabilities that cannot be remediated by OIT at the enterprise level are referred to OIT staff assigned to specific facilities for action. The OIG inspection team examined whether the Spokane Healthcare System identified and remediated vulnerabilities within established times and configured its servers according to standards.

Finding 1: The Healthcare System Had Two Deficiencies in Configuration Management

The team concluded that the healthcare system had deficiencies in two configuration management controls:

- **Vulnerability remediation.** Analysis of the OIT's vulnerability scan results and its plans of action and milestones showed the facility did not always create plans of action and milestones for vulnerabilities persisting past the 60-day limit set by VA.[14]
- **System baseline configurations.** The OIG team found the healthcare system was not always using secure baseline configurations.

[13] Firmware refers to software that is embedded in the read-only memory of hardware; it enables the hardware to function and communicate with other software. GAO, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-24-107026, September 2024.

[14] In April 2024, VA increased the time to remediate critical vulnerabilities from 30 days to 60 days. VA's Information Security Knowledge Service, "Security Controls Explorer," April 9, 2024.

Vulnerability Remediation

FISMA audits have repeatedly found deficiencies in VA's vulnerability management controls. Consistent with those findings, the team identified deficient controls at the VA Spokane Healthcare System. A vulnerability is a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source."[15]

Vulnerability management is how an organization identifies, classifies, and reduces weaknesses. It also helps the organization assess risks and monitor the effectiveness of its overall security program. At VA, OIT conducts both 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 stewards responsible for entering all critical- and high-severity vulnerabilities that cannot be remediated on time (within 60 days) into a plan of action and milestones for remediation.[16] Information stewards should then use a prescribed form to provide evidence showing that the deficiencies have been mitigated.[17]

NIST guidance calls for a severity level to be assigned to each vulnerability using the Common Vulnerability Scoring System.[18] The inspection team's testing of vulnerability remediation focused on whether critical and high vulnerabilities were remediated within agency-approved timelines, as shown in table 2.

[15] GAO, *FISCAM*.

[16] 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, or critical based on various factors including attack complexity, the ability to perform an attack remotely, the privileges required, the impact of the attack, and the availability and sophistication of exploit tools.

[17] According to the NIST Computer Security Resource Center Glossary, an information 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 June 9, 2025, https://csrc.nist.gov/glossary/term/information_steward.

[18] "Vulnerability Metrics" (web page), NIST National Vulnerability Database, accessed June 9, 2025, https://nvd.nist.gov/vuln-metrics/cvss; "Common Vulnerability Scoring System ver. 4.0, Specification Document, Version 1.2," Forum of Incident Response and Security Teams, accessed June 9, 2025, https://www.first.org/cvss/v4-0/cvss-v40-specification.pdf.

Table 2. Vulnerability Remediation Timelines by Severity Level

Severity score	Severity level	OIT time to remediate
9.0–10	Critical	60 days
7.0–8.9	High	60 days

Source: VA OIG analysis of VA's Information Security Knowledge Service, "Security Controls Explorer," February 18, 2025.

Note: The Knowledge Service is the approved source for VA cybersecurity and privacy policies, procedures, processes, and guidance.

The inspection team compared the results of the OIT-provided network vulnerability scan from the VA Spokane Healthcare System against OIG scans conducted from January 27 through February 5, 2025. OIT and the inspection team used the same vulnerability scanning tools. The OIG found no material differences between the two network scans. Both scans showed a high number of vulnerabilities persisting past deadlines.

As of February 2025, the Spokane Healthcare System had multiple critical and high vulnerabilities identified across numerous systems that were not remediated within the required deadlines and for which no one had developed plans of action or milestones. Additionally, OIG scans identified several high-risk vulnerabilities.

System Baseline Configuration

During the inspection, the team also scanned the configurable settings of the healthcare system's core network device and multiple databases 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 on by managers. However, certain software configuration settings did not meet baseline security requirements.

The OIG team identified specific security configuration deficiencies and communicated them to VA to address. Given the potential severity of such failures, the security configuration of servers is not just a defensive strategy but a proactive one that helps protect the confidentiality, availability, and integrity of VA systems.

Finding 1 Conclusion

Numerous system vulnerabilities were not mitigated on time, and software did not meet baseline requirements. These security weaknesses on the VA Spokane Healthcare System's network present a risk of unauthorized access to sensitive information or disruption to operations.

Recommendations 1–2

The OIG made two recommendations to the assistant secretary for information and technology and chief information officer:[19]

1. Implement vulnerability management processes to ensure all vulnerabilities are identified and plans of action and milestones are created for vulnerabilities that cannot be mitigated by VA deadlines.
2. Implement a more effective baseline configuration process to ensure network devices and databases are running authorized software that is configured to approved baselines and free of vulnerabilities.

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

VA Management Comments

In December 2025, the Deputy Secretary of VA, performing the delegable duties of the acting assistant secretary for information and technology, concurred with recommendations 1 and 2. For recommendation 1, he stated that OIT addressed the vulnerabilities identified in the OIG's January 2025 scan, and either remediated or documented all vulnerabilities in a plan of action and milestone item. As a result, VA requested that recommendation 1 be closed. In response to recommendation 2, the Deputy Secretary indicated OIT completed a change order to bring the core network switch configuration into compliance with VA's security baseline and will complete additional remediation actions. The full text of the Deputy Secretary's response is included in appendix D.

OIG Response

The planned corrective actions are responsive to the intent of the recommendations. For recommendation 1, actions were taken to provide agency oversight into the vulnerabilities on the network, but there are still vulnerabilities that need plans of action and milestones based on the evidence provided. Therefore, the OIG considers recommendation 1 open. The OIG will monitor implementation of the planned actions and will close recommendations 1 and 2 when VA provides evidence demonstrating progress in addressing the identified issues.

[19] 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.

II. Security Management

According to *FISCAM*, security management controls establish a framework and a continuous cycle for managing risk, developing security policies, and monitoring the effectiveness of procedures. The inspection team evaluated EHR user management controls at the Spokane Healthcare System.

To assess security management 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 the information system security officers, biomedical staff, and the area manager. The team also conducted a walk-through of the Mann-Grandstaff VA Medical Center. Security management controls reviewed included user management.

Finding 2: The Healthcare System Had One Deficiency in Security Management

The inspection team identified one deficiency with security management at the Spokane Healthcare System, as described below.

Evaluation of Access Controls to Ensure Security of PII

The OIG identified some VA users (including volunteers and scheduling clerks) with access to the federal EHR who maintained unnecessary access to an EHR screen that contained unredacted PII.[20] A business operations supervisor told the inspection team that access was originally granted because there was a need to obtain individual records from a legacy system; but this access to unredacted PII was no longer needed.

The OIG team identified the individuals in the Spokane Healthcare System who had access to veterans' PII via unredacted fields in the EHR demographic screen and communicated that information to VA. Additionally, the team identified similar users of other VA healthcare systems with the federal EHR, including volunteers and scheduling clerks, who had access to the unredacted PII within the EHR. NIST allows agencies flexibility to remove, mask, encrypt, or replace PII.[21] A compromise of PII could result in a veteran facing social, economic, or physical

[20] GAO, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, GAO-08-536 May 2008. GAO defines PII as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

[21] NIST Special Publication 800-53 revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020.

harm. Additionally, a breach of PII would result in a financial and reputational loss to VA, which is entrusted to protect sensitive veteran data.

Finding 2 Conclusion

Some individuals at the VA Spokane Healthcare System maintained unnecessary access to an EHR screen that contained unredacted PII. This presented an unnecessary risk of exposing veterans' personal information.

Recommendation 3

The OIG made one recommendation to the assistant secretary for information technology and chief information officer, along with the program executive director of the Electronic Health Record Modernization Integration Office:[22]

3. Perform a cost-benefit analysis and implement appropriate controls within the federal Electronic Health Record to limit disclosure of veteran personally identifiable information based on job responsibility.

VA Management Comments

The Deputy Secretary of VA, performing the delegable duties of the assistant secretary for OIT, concurred with recommendation 3. He responded that the disclosure of PII to VA staff and volunteers for care purposes complies with Veterans Health Administration Directive 1605.02, with standardized EHR roles, required annual training, and reasonable measures to limit incidental exposure. He further stated the federal EHR uses predefined, standardized, curated user roles, and the practice follows the "need to know" principle.

Still, the Deputy Secretary stated the Electronic Health Record Modernization Integration Office will coordinate with relevant stakeholders to conduct an impact analysis of user role access within the EHR system. He stated the analysis will assess the risks and operational impacts of PII disclosure, and the findings will guide the implementation of security controls to limit disclosure. The full text of the Deputy Secretary's response is included in appendix D.

OIG Response

For recommendation 3, the planned corrective actions are responsive to the intent of the recommendation. The OIG will monitor implementation of the planned actions and will close the recommendation when VA provides evidence demonstrating progress in addressing the identified issue.

[22] The recommendations are directed to anyone in an acting status or performing the delegable duties of the positions.

III. Access Controls

Previous FISMA reports have repeatedly identified access controls as a nationwide issue for VA. Access controls—including boundary protections, sensitive system resources, physical security, and audit and monitoring controls—provide reasonable assurance that computer resources are restricted to authorized individuals.[23] Access controls can be both logical and physical:

- **Logical access controls** require users to authenticate themselves, limit the resources that users can access, and restrict the actions users can take.
- **Physical access controls** restrict physical and logical access to computer resources to protect them from loss or impairment.

Identification, authentication, and authorization controls ensure users have proper access and that access is restricted to authorized individuals. The inspection team reviewed access and environmental controls over the computer room and communications closets at the Mann-Grandstaff VA Medical Center in Spokane.[24] To evaluate the Mann-Grandstaff 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.

Finding 3: The Healthcare System Had Four Deficiencies in Access Controls

The OIG found issues with the management of keys, unsecured network equipment, electrical grounding, and fuel storage.

Management of Physical Facility Keys

The inspection team discovered that physical access to the facility and its IT resources was not effectively controlled. Although the facility had a process for assigning physical keys, the same individuals who could create keys also maintained the blank key stock, allowing them to potentially make unauthorized keys. Segregation of duties is a fundamental security principle to prevent unauthorized access. Additionally, the lack of an inventory for blank key stock made it impossible to detect whether unauthorized keys were made, highlighting the need for separation of duties to prevent misuse.

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

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

Unsecured Network Equipment

The OIG found that network infrastructure was not properly secured at two locations. Although the equipment was not in a public area of the facility, it was not secured in a communications closet or approved enclosure that would restrict access to only authorized personnel, as required.[25]

Electrical Grounding

The OIG tested 31 of the 36 communications closets at the Mann-Grandstaff VA Medical Center and found that 11 did not meet federal and VA environmental security requirements related to the grounding of equipment.[26] Staff at the facility were unaware that equipment was not properly grounded. Without proper grounding, the equipment could be damaged by electromagnetic interference, a power surge, or electrostatic discharge. Additionally, not having a proper grounding network could reduce the ability for facilities to provide health care, negatively affecting patient health.

Fuel Storage

During a tour of the facility, the OIG team determined that a tank at a fueling station did not meet VA control guidelines for having adequate anti-ram barriers.[27]

Finding 3 Conclusion

The Spokane Healthcare System's access controls did not appropriately restrict access to facility keys that were protecting computer resources, leaving them unprotected from theft and intentional or accidental damage. Additionally, environmental controls were not consistently implemented to safeguard equipment in communications closets and the fueling station. If the deficiencies are not corrected, the healthcare system risks unauthorized access, disruption, and destruction of critical resources.

Recommendations 4–7

The OIG made four recommendations to the VA Spokane Healthcare System's director, along with the assistant secretary for information and technology:[28]

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

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

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

[28] The recommendations are directed to anyone in an acting status or performing the delegable duties of the positions.

4. Segregate the duties of maintaining key stock and making keys.
5. Place network infrastructure equipment in a communications closet or approved enclosure to restrict access to only authorized personnel.
6. Complete the installation of grounding measures for all telecommunications closets to protect information technology equipment against electromagnetic pulse attack or electrostatic discharge. Ensure the work completed by contractors adheres to the requirements as defined in the work order.
7. Add anti-ram barriers to protect all sides of a fueling station's fuel tank.

VA Management Comments

The Deputy Secretary of VA, performing the delegable duties of the assistant secretary for information and technology, concurred with recommendations 4, 5, 6, and 7. For recommendation 4, he reported that the Spokane Healthcare System is developing a policy to separate the duties of maintaining key stock and making keys.

In response to recommendation 5, he stated the healthcare system remediated one rack by installing a new cabinet and has funded a project to remediate the second rack. For recommendation 6, the Deputy Secretary indicated the facility will request to design and execute physical upgrades needed to meet federal and VA requirements and, in the interim, placed the servers in a secure room with restricted access.

Finally, to address recommendation 7, he stated Spokane Healthcare System verified that the fuel tank in question was empty and additional concrete blocks were installed to further mitigate risk. The full text of the Deputy Secretary's response is included in appendix D.

OIG Response

The corrective actions are responsive to the intent of the recommendations. Based on the actions already taken and evidence provided by VA, the OIG considers recommendation 7 closed. The OIG will monitor implementation of the remaining planned actions and will close recommendations 4, 5, and 6 when VA provides evidence demonstrating progress in addressing the identified issues.

Appendix A: Recommendations from FISMA Audit for FY 2024 Report

In the Federal Information Security Modernization Act of 2014 (FISMA) audit for fiscal year 2024, CliftonLarsonAllen LLP made 23 recommendations.[29] Of the 23 recommendations, 21 were repeat recommendations from the prior year.[30] The FISMA audit assesses the VA-wide security management program, and recommendations in the FISMA report are not specific to the VA Spokane Healthcare System.

Recommendations 6 and 7 were made to the Office of Personnel Security, Human Resources, and Contract Offices.[31] The other 21 recommendations were made to the assistant secretary for information and technology. All recommendations are reprinted below:

1. Consistently implement an improved continuous monitoring program in accordance with the National Institute of Standards and Technology's Risk Management Framework. Specifically, regarding the independent evaluation of the effectiveness of security controls prior to granting authorization decisions.
2. Implement improved processes for reviewing and updating key security documentation, including Security Control Assessments, Risk Assessments, and Privacy Impact Assessments as needed. Such updates will ensure all required information is included and accurately reflects the current environment, new security risks, and applicable federal standards.
3. Implement improved processes to ensure System Security Plans reflect the status of security control implementations and risks are accurately reported to support a comprehensive risk management program across the organization.
4. Coordinate with system owners and local system management to ensure the consistent monitoring and reviewing of privileged accounts, service accounts, and accounts for individuals with access to source code repositories are performed across VA systems and platforms.
5. Implement measures to ensure that system stewards and other officials responsible for system-level plans of action and milestones are closing items with relevant support that shows sufficient remediation of the identified weakness.

[29] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2024*, Report No. 24-01233-90, June 18, 2025.

[30] Recommendations 11 and 16 were new in 2024.

[31] The deputy chief information officer, connectivity and collaboration services, performing the delegable duties of the assistant secretary for information and technology and chief information officer, responded to recommendations 6 and 7.

6. Strengthen processes to ensure appropriate levels of background investigations are performed timely and completed for applicable VA employees and contractors.
7. Implement improved processes for establishing and maintaining accurate investigation data within VA systems used for background investigations.
8. Ensure contingency plans for all systems and applications are updated and tested in accordance with VA requirements.
9. Implement improved procedures to ensure that system outages are resolved within stated recovery time objectives.
10. Ensure system owners consistently implement processes for periodic reviews of user account access. Remove unnecessary and inactive accounts on systems and networks.
11. Ensure the consistent monitoring and reviewing of privileged accounts, service accounts, and accounts for individuals with access to source code repositories are performed across VA systems and platforms.
12. Implement improved processes to ensure compliance with VA password policy and security configuration baselines on domain controllers, operating systems, databases, applications, and network devices.
13. Ensure established change control procedures are consistently followed for testing and approval of system changes for VA applications and networks.
14. Continue to implement and consistently enforce established procedures for preventing and detecting potential unauthorized changes across all platforms and applications in the environment.
15. Ensure that all systems and platforms are monitored for compliance with documented VA standards for baseline configurations. Ensure that system owners consistently implement and monitor their configurations.
16. Implement automated software management processes on all agency platforms to identify and prevent the use of unauthorized software on agency devices.
17. Implement improved procedures for establishing, documenting, and monitoring an accurate software and logical hardware inventory for system boundaries across the enterprise.
18. Implement improved processes for monitoring and analyzing significant system audit events for unauthorized or unusual activities across all systems and platforms in accordance with VA policy. Ensure privileged activity is monitored on all systems and applications.

19. Enable system audit logs on all critical systems and platforms and conduct centralized reviews of security violations across the enterprise.
20. Implement improved mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and Web application servers in accordance with established policy time frames. If patches cannot be applied or are unavailable, other protections or mitigations should be documented and implemented to address the specific risks.
21. Implement improved segmentation controls that restrict vulnerable medical devices from unnecessary access from the general network.
22. Implement improved processes to require system owners and management to provide adequate credentials to ensure security scans are authenticated to end devices where feasible and the subsequent vulnerabilities are remediated in a timely manner.
23. Improve the process for tracking and resolving vulnerabilities that cannot be addressed by enterprise processes within policy time frames. Implement mitigations for identified security deficiencies by applying security patches, system software updates, or configuration changes to reduce applicable security risks.

Appendix B: Background

Federal Information Security Modernization Act (FISMA) of 2014

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 (NIST) Security Guidelines

NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems.[32] It develops information security standards and guidelines in 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.

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

Federal Information System Controls Audit Manual (FISCAM)

The Government Accountability Office developed the *FISCAM,* a methodology for evaluating the confidentiality, integrity, and availability of information systems. The *FISCAM* groups information categories of similar risks into the following six broad categories: business process controls, security management, access controls, configuration management, segregation of duties, and contingency planning.[33] To help auditors evaluate information systems, the *FISCAM* aligns control categories with NIST controls.

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

Appendix C: Scope and Methodology

Scope

The VA Office of Inspector General (OIG) inspection team conducted its work from January through August 2025. 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 (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 Spokane Healthcare System and its information systems for security compliance. Additionally, the team interviewed VA staff responsible for the healthcare system's information technology security and operations and conducted an on-site physical security review of the Mann-Grandstaff VA Medical Center. To determine local systems' security compliance, the team conducted vulnerability and configuration testing for the VA Spokane Healthcare System at the VA Mann-Grandstaff VA Medical Center. 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 internal controls were significant to the inspection's objectives. The overall scope of information security inspections is the evaluation of general security and application controls that support VA's programs and operations. According to the risk management framework for VA information systems, the information security program is the foundation for VA's information security and privacy program and practices. The framework is documented in VA Handbook 6500.

The team used the Government Accountability Office's (GAO) *Federal Information System Controls Audit Manual (FISCAM)* as a template to plan the inspection. When planning for this inspection, the team identified potential information system controls that would significantly affect the review. Specifically, the team used the *FISCAM*'s appendix II as a guide to help develop evidence requests and interview questions. The team used the *FISCAM* controls identified in appendix B of this report to determine the FISMA controls VA uses 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,

some controls overlap and are included in both assessments due to redundant roles and responsibilities among VA's local, regional, and national facilities and offices.

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

Data Reliability

The inspection team generated computer-processed data by using network scanning tools. The results of the scans were provided to the Office of Information and Technology. The team used an industry-standard information system security tool to identify information systems on the VA network and to capture relevant configuration information. This tool is used to identify vulnerabilities and compliance with secure baselines. 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. If the system did not have the current software version, the tool identified that as a vulnerability. 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*.

Appendix D: VA Management Comments

Department of Veterans Affairs Memorandum

Date: December 11, 2025

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, Inspection of Information Security at the VA Spokane Healthcare System in Washington (VIEWS 13614889)

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, *Inspection of Information Security at the VA Spokane Healthcare System in Washington* (Project Number 2025-00975-AE-0046). The Office of Information and Technology (OIT) concurs with OIG's recommendations and submits the attached action plan.

2. 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 seven recommendations, of which OIT concurs with all seven. OIT is providing a corrective action plan and target implementation date for recommendations 2-6, and closure evidence demonstrating OIT has addressed the identified issues for recommendations 1 and 7.

The OIG removed point of contact information prior to publication.

(Original signed by)

Paul R. Lawrence, PhD

Attachment

Attachment

Office of Information and Technology

Comments on Office of Inspector General Draft Report,

Inspection of Information Security at the VA Spokane Healthcare System

in Washington

Project Number 2025-00975-AE-0046

Recommendation 1: Improve existing vulnerability management processes to ensure all vulnerabilities are identified and plans of action and milestones are created for vulnerabilities that cannot be mitigated by VA deadlines.

Comments: Concur. The Department of Veterans Affairs (VA) Office of Information and Technology (OIT) addressed the vulnerabilities identified in the Office of Inspector General's January 2025 scan, with all vulnerabilities either remediated or documented in a plan of action and milestone item.

Expected Completion Date: Completed, July 29, 2025.

VA requests closure of recommendation 1.

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

Comments: Concur. OIT completed a change order to bring the core network switch configuration into compliance with the VA security baseline. OIT will complete additional remediation actions by January 2026.

Expected Completion Date: January 31, 2026.

Recommendation 3: Perform a cost benefit analysis and implement appropriate controls within the Federal Electronic Health Record to limit disclosure of veteran PII based on job responsibility.

Comments: Concur. The disclosure of Veterans' and patients' Personally Identifiable Information (PII) to VA employees for purposes of healthcare treatment, health care operations, and continuity of care is consistent with the Veterans Health Administration (VHA) Directive 1605.02, Minimum Necessary Standard for Access, Use, Disclosure, and Requests of Protected Health Information (PHI), dated April 4, 2019. Volunteers are considered unpaid VA employees. All VA users, including scheduling clerks and volunteers, must complete the mandated annual security and privacy training courses appropriate to their roles before being granted access to Federal Government computer systems.

VA's legacy Computerized Patient Record System allows a user to add, remove, and otherwise customize permissions for each user based on that user's needs. In contrast, Oracle Health's Millennium electronic health record (EHR), the core component of VA's Federal EHR, uses pre-defined, standardized, curated user roles at the national/enterprise level. This practice follows the "need to know" principle for user provisioning and is compliant with VHA Directive 1605.02. Generally, redacting PII/PHI from EHR screens is not appropriate, as it may impact on the staff's ability to perform necessary functions. While staff should only access the minimum information necessary to perform their official duties, incidental use or disclosure of PII may occur while providing health care. For example, certain EHR screens may display information to multiple roles, even if not all users require access to that data. One position may not need that information, but total customization of every field on every screen is not

feasible. However, if reasonable measures are in place to limit incidental disclosure, no privacy violation occurs.

Nevertheless, the EHR Modernization Integration Office will coordinate with relevant stakeholders to conduct an impact analysis of user role access within the Federal EHR system. This analysis will assess the risks and operational impacts of PII disclosure, and the findings will guide the implementation of security controls to limit disclosure.

Expected Completion Date: January 31, 2026.

Recommendation 4: Segregate the duties of maintaining key stock and making keys.

Comments: Concur. The VA Spokane Healthcare System is developing a policy to separate the duties of maintaining key stock and making keys.

Expected Completion Date: January 31, 2026.

Recommendation 5: Place network infrastructure equipment in a communication closet or approved enclosure to restrict access to only authorized personnel.

Comments: Concur. The VA Spokane Healthcare System remediated one rack by installing a new cabinet. The facility has funded a project to remediate the second rack by moving it to a secure information technology closet.

Expected Completion Date: January 31, 2026.

Recommendation 6: Complete the installation of grounding measures for all telecommunication closets to protect information technology equipment against electromagnetic pulse attack or electrostatic discharge. Ensure the work completed by contractors adheres to the requirements as defined in the work order.

Comments: Concur. The facility will submit a request through the Strategic Capital Investment Process to design and execute physical upgrades needed to meet Federal and VA requirements. To ensure interim protection, the servers are in a secure room with restricted access. Additionally, these secure rooms are located on a VA campus that is monitored by a 24-hour police presence.

Expected Completion Date: September 30, 2028.

Recommendation 7: Add anti-ram barriers to protect all sides of the fueling station's fuel tank.

Comments: Concur. The VA Spokane Healthcare System verified that the fueling station's tank is empty of fuel. To further mitigate risk, the facility installed additional concrete blocks.

Expected Completion Date: Completed, July 24, 2025.

VA requests closure of recommendation 7.

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 Sachin Bagai Nicholas Hartzheim Kimberly Moss Albert Schmidt
Other Contributors	Georgina Baumgartner Justin Skeen Rashiya Washington

Report Distribution

VA Distribution

Office of the Secretary
Office of the Deputy 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
Electronic Health Record Modernization Integration Office
VA Spokane Healthcare System
VISN 20: Veterans Integrated Services Network

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
  Idaho: Mike Crapo, James E. Risch
  Montana: Steve Daines, Tim Sheehy
  Washington: Maria Cantwell, Patty Murray
US House of Representatives
  Idaho: Russ Fulcher
  Montana: Ryan Zinke
  Washington: Michael Baumgartner, Dan Newhouse, Kim Schrier

OIG reports are available at [www.vaoig.gov.](http://www.vaoig.gov)