US DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

DEPARTMENT OF VETERANS AFFAIRS

Inspection of Information Security at the Lovell Federal Healthcare System in Illinois

Information Security Inspection	**25-04267-174**	**September 10, 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 an inspection of the Lovell Federal Healthcare System in Illinois to assess compliance with federal cybersecurity standards under the Federal Information Security Modernization Act (FISMA).[1] The inspection focused on three security control categories: configuration management, security management, and access control. The OIG selected the Lovell Federal Healthcare System because it had not been visited as part of an annual FISMA audit since 2017.

The OIG visited the Captain James A. Lovell Federal Health Care Center in North Chicago, Illinois, in January 2026. The OIG communicated with VA staff throughout the inspection. In February 2026, the facility corrected a security management deficiency after the team notified facility staff of the issue. In March 2026, the OIG provided VA with details of its preliminary findings and recommendations. 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 report, the OIG made seven recommendations to strengthen configuration management and improve network and physical security. These deficiencies could compromise the protection of VA data and information systems from unauthorized access, alteration, or destruction. As of June 2026, VA's Office of Information and Technology (OIT) provided sufficient evidence that it had fully addressed two of the seven recommendations. Accordingly, recommendations 1 and 4 are considered closed. In July 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 seven recommendations. OIT provided corrective action plans for the remaining open recommendations.

What the Inspection Found

The OIG team identified deficiencies in all three control areas inspected. For configuration management, the OIG concluded that VA staff did not remediate multiple high- and critical-severity vulnerabilities within VA-defined time frames and had not developed required action plans. Additionally, some devices were not configured according to approved security baselines. These issues increase the risk of unauthorized access and operational disruption.

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

Regarding security management, the OIG identified one issue that put veterans' personal data at risk. The healthcare system did not follow VA requirements for setting access to the Electronic Health Record and network accounts to be automatically removed for temporary staff.

For access controls, the OIG identified five deficiencies. Not all networked medical devices or special-purpose systems in the healthcare system were protected by being isolated on the parts of the network that they reside on. Weak controls over physical key distribution allowed for the potential creation of unauthorized keys, and gaps in backup power across communications areas threatened continued service during outages. Additionally, not all communications closets met federal and VA environmental security requirements related to the grounding of equipment. Last, a witness did not always observe the destruction of temporary paper records that contained personally identifiable information. These issues are threats to operations, data integrity, and VA's reputation.

Next Steps

The OIG will continue to evaluate OIT's actions and will close the remaining five recommendations once OIT 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
IT	information technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information and Technology
OMB	Office of Management and Budget

Introduction

Information security controls protect VA systems and data from unauthorized access, use, modification, or destruction.[2] The VA Office of Inspector General (OIG) conducts information security inspections that provide specific recommendations to VA on enhancing information security oversight at local and regional facilities. They are typically conducted at selected facilities that have not recently been assessed in an annual Federal Information Security Modernization Act of 2014 (FISMA) audit or have previously performed poorly.[3] Appendix A provides more detail on this inspection's scope and methodology.

The OIG conducted this inspection to determine whether the Lovell Federal Healthcare System in Illinois was meeting federal security guidance. The OIG selected this healthcare system because it had not been visited as part of the annual FISMA audit since 2017. The OIG also noted that the Lovell Federal Healthcare System transitioned to the federal Electronic Health Record (EHR) in March 2024.[4] The OIG team visited the Captain James A. Lovell Federal Health Care Center in North Chicago, Illinois, in January 2026.

In February 2026, after the team notified the facility of the one security management deficiency found, the facility corrected the issue; as a result, the OIG did not make a related recommendation. In March 2026, the OIG provided OIT with details of its preliminary findings and recommendations related to this inspection containing "VA sensitive data" as defined in 38 U.S.C. § 5727. Federal law, including FISMA and its implementing regulations, requires federal agencies to protect sensitive data and information systems due to the risk of harm that could result from improper disclosure. Accordingly, that internal material is not being published by the OIG or distributed outside VA.

This report provides findings and recommendations that are specific to the Lovell Federal Healthcare System, but other facilities across VA could benefit from reviewing this information and considering the OIG's recommendations.

Security Controls

The National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) provide criteria for implementing security controls. NIST establishes security and

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

[3] Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014); VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2024*, Report No. 24-01233-90, June 18, 2025.

[4] "EHR Deployment Schedule" (web page), VA, https://digital.va.gov/ehr-modernization/ehr-deployment-schedule/, accessed November 19, 2025.

privacy controls for systems to help organizations identify the controls needed to manage risk and to satisfy federal security and privacy requirements.[5] According to OMB, security and privacy control assessments ensure that controls selected by agencies are implemented correctly, operate as intended, and effectively satisfy security and privacy requirements.[6] Appendix B presents information about FISMA and other federal criteria and standards discussed in this report.

The assistant secretary for information and technology, who is also the VA 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 (IT).[7] 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.[8]

This OIG information security inspection focused on three selected security control areas identified in the *Federal Information System Controls Audit Manual* (*FISCAM*), as shown in table 1 on the next page. *FISCAM* groups related NIST security and privacy controls into categories that have similar types of risks. Weaknesses in these controls can result in unauthorized access to, modification of, or disclosure of VA sensitive data and programs and disruption of critical operations.[9]

[5] NIST Special Publication 800-53.

[6] OMB Circular A-130.

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

[8] VA Handbook 6500.

[9] 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 configuration, vulnerability monitoring and scanning, and system and information integrity
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	Policies and procedures, and risk response
Access	Limit access to information resources and detect inappropriate access	Access controls, audit and accountability, physical and environmental protection, and system and communication protection

Source: FISCAM and VA OIG analysis.

Office of Information and Technology Structure and Responsibilities

The assistant secretary for information and technology serves as chief information officer and leads the Office of Information and Technology (OIT).[10] OIT's end user operations team provides on-site support to IT customers across all VA administrations and program offices—including VA employees and contractors with government-furnished IT equipment.[11] End user operations staff assigned to the Lovell Federal Healthcare System are responsible for managing system plans of action and milestones to ensure all assessed and scanned vulnerabilities are documented.[12] The Cybersecurity Operations Center, part of the Office of Information Security, serves as the authoritative source for addressing and managing cybersecurity incidents.[13]

Results of Previous Projects

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

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

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

[12] 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.

[13] VA Handbook 6500.

management, security management, and access controls. This inspection evaluates local implementation of these control areas at the Lovell Federal Healthcare System.[14]

Lovell Federal Healthcare System

The Lovell Federal Healthcare System consists of the Captain James A. Lovell Federal Health Care Center and the Evanston, Kenosha, and McHenry outpatient clinics. The healthcare center is a partnership between VA and the Department of Defense that provides healthcare services to active-duty military, their family members, military retirees, and veterans.

According to the healthcare system's department head of patient administration, in fiscal year 2025, the healthcare center provided care to more than 81,000 patients. He also provided the OIG team with documentation that the healthcare center had 3,235 employees (2,390 from VA and 845 from the Department of Defense) and a budget of more than $823.8 million (with $594.8 million in VA funds and $229 million in Department of Defense funds).

[14] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2024*; 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 OIG team visited the Captain James A. Lovell Federal Health Care Center in North Chicago, Illinois, in January 2026. The team assessed configuration management, security management, and access controls and found that improvements are needed in all three control areas. The OIG made seven recommendations to enhance OIT's processes and improve adherence to laws protecting veterans' information and VA data and information systems. As of June 2026, OIT provided sufficient evidence that it had fully addressed two of the seven recommendations, and the OIG closed them. The OIG will evaluate OIT's actions and will close the remaining recommendations once OIT provides complete documentation and sufficient evidence that it has addressed the intent of the recommendations and the issues identified in this report.

I. Configuration Management

According to GAO's *FISCAM*, configuration management involves identifying and managing security features for IT such as hardware, software, and firmware at a given point and systematically controlling changes to that configuration during the system's operation. NIST Special Publication 800-128 notes that an effective configuration management process is essential to the security of information and systems.[15] At the Lovell Federal Healthcare System, the OIG team evaluated selected NIST controls relevant to configuration management.[16]

To evaluate this control area, the team interviewed staff from OIT, facility management, and information system security; reviewed policies and procedures; conducted walk-throughs of the facility; assessed scan results from OIT; independently scanned local network devices for vulnerabilities and compliance; and analyzed evidence. See appendix A for more information about the inspection's scope and methodology.

Finding 1: The Lovell Federal Healthcare System Had Two Configuration Management Deficiencies

The OIG team concluded that the healthcare system had two deficiencies in configuration management controls. The team's 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.[17] 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.

[15] NIST, Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011.

[16] NIST Special Publication 800-53.

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

Vulnerability Remediation

FISMA audits have repeatedly found deficiencies in VA's vulnerability management controls. Similar to those findings, the OIG team identified deficient controls at the Lovell Federal Healthcare System. According to GAO's *FISCAM*, 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."

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. NIST guidance calls for vulnerabilities to be given a severity level based on the Common Vulnerability Scoring System developed by the Forum of Incident Response and Security Teams, an international consortium of security and incident-response organizations.[18] The system provides a numerical score ranging from low to medium, high, or critical severity 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 tools that could exploit the vulnerabilities.

In 2023, OIT implemented a formal process to track the monitoring and remediation of vulnerabilities by using a plan of action and milestones. This tracking process makes agency officials who have statutory or operational authority responsible for entering all high- and critical-severity vulnerabilities that cannot be remediated within required timelines into a plan of action and milestones for remediation. These officials should then document evidence showing the deficiencies have been mitigated. The OIG team's testing of vulnerability remediation focused on whether critical- and high-severity vulnerabilities were remediated within the agency-approved timeline.[19]

The OIG found no material differences between the OIT-provided network vulnerability scan and the OIG scans. Both showed a high number of vulnerabilities persisting past deadlines. Specifically, as of January 2026, the Lovell Federal Healthcare System had multiple high- and critical-severity vulnerabilities identified across numerous systems that were not remediated within the required timelines and for which no one had developed plans of action and milestones. Plans of action and milestones are used to document resources and actions needed to remediate the vulnerabilities. These vulnerabilities had not been remediated as part of OIT's automated patch management program.

[18] "Vulnerability Metrics" (web page), NIST National Vulnerability Database, accessed July 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 July 9, 2025, https://www.first.org/cvss/v4-0/cvss-v40-specification.pdf.

[19] VA's Information Security Knowledge Service, "Security Controls Explorer," updated April 9, 2024.

OIT's Cybersecurity Operations Center director told the OIG team that they plan to prioritize remediation for internet-facing hosts, which they said are protected by perimeter controls. This plan will help protect internet-facing devices from external threats; however, it does not fully address risks associated with insider threats, including hosts owned or managed by contractors. The director also said the center is developing a process to automate the creation of plans of action and milestones, and he reported plans to establish a process demonstrating how systems will transition to vulnerability-free software versions.

System Baseline Configuration

The team also checked compliance with secure baseline configurable settings for a core network device and some databases that support the healthcare system. According to VA Handbook 6500 (which outlines procedures for the risk management framework for VA information systems), these settings should be configured using baselines that have been documented, formally reviewed, and agreed upon by managers. However, the OIG found that certain software configuration settings did not meet baseline security requirements. The OIG team communicated these deficiencies for VA to address. Given the potential severity of the impact of not using secure baselines, securely configured servers are 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 weaknesses in vulnerability tracking and system configuration put veterans' data and VA's healthcare operations at serious risk of unauthorized access. They also could affect the availability of VA systems, causing operational disruptions.

Recommendations 1–2

The OIG made the following recommendations to the assistant secretary for information and technology, who also serves as chief information officer:[20]

1. Improve vulnerability management processes so that all vulnerabilities are identified and mitigated; for vulnerabilities that cannot be mitigated by VA deadlines, create plans of action and milestones.
2. Improve the baseline configuration process to make sure network devices and databases are running authorized software that is configured to approved baselines and free of vulnerabilities.

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

VA Management Comments

The VA Deputy Secretary, performing the delegable duties of the acting assistant secretary for information and technology and chief information officer, concurred with both recommendations. For recommendation 1, the healthcare system remediated or formally documented all identified vulnerabilities in a plan of action and milestones within the applicable VA policy time frames in place at the time of the audit. For recommendation 2, he said the healthcare system is improving its monitoring and remediation processes to identify and address configuration deviations and vulnerabilities promptly, reducing cybersecurity risk and supporting compliance with applicable security requirements. The full text of the Deputy Secretary's response is included in appendix C.

OIG Response

Based on the evidence of corrective actions provided by VA in June 2026, the OIG considers recommendation 1 closed. The corrective action plan for recommendation 2 is responsive to the intent of the recommendation. The OIG will monitor implementation of the planned actions and will close recommendation 2 when VA provides evidence demonstrating it has addressed the identified issue.

II. Security Management

According to *FISCAM*, security management controls establish a framework and a continuous cycle for managing risk, developing security procedures, and monitoring the effectiveness of the controls. To evaluate this control area, the OIG team assessed applicable policies and procedures and risk response. The team also interviewed staff from OIT, facility management, and information system security and privacy; reviewed local policies and procedures; conducted walk-throughs of the facility; and analyzed evidence. See appendix A for more information about the inspection's scope and methodology.

Finding 2: The Lovell Federal Healthcare System Had One Security Management Deficiency

The OIG team identified one deficiency in security management controls. The healthcare system did not follow VA requirements for setting access to EHR and network accounts to be automatically removed for temporary staff once they are no longer working at VA.

Access to Accounts

The OIG determined the healthcare system did not set access to network accounts to be automatically removed for temporary staff (specifically, student accounts) in line with VA and federal requirements.[21] To access the EHR, users need a VA network and EHR account. The OIG team found that not all network accounts belonging to temporary staff were set to be disabled, and some had expiration dates assigned to the network account that greatly exceeded the expected end date of the staff's work agreement. An individual who retains access after separation could obtain information for unauthorized disclosure or modify information in the system that could affect care or operations. Additionally, retained access could cause a breach of personal health information, leading to financial or reputational loss for VA.

In February 2026, after the OIG team notified the facility of this issue, facility staff entered correct expiration dates for individuals. They also created standard operating procedures for establishing appropriate expiration dates for these temporary accounts.

Finding 2 Conclusion

The healthcare system did not follow VA requirements for setting access to the EHR and for automatically removing temporary staff network accounts. This could affect veteran care or the healthcare system's operations. It could also result in a breach of personal health information,

[21] VA Information Security Knowledge Service, "Security Controls Explorer," April 29, 2025; *End User Services End User Operations Security Controls—Access Control (AC) Standard Operating Procedures (SOP)*, March 8, 2023; NIST Special Publication 800-53.

which could lead to a financial and reputational loss to VA, an agency entrusted to protect sensitive veteran data.

Based on the evidence of corrective actions provided by VA in February 2026, the OIG did not make a recommendation for this finding.

III. Access Controls

According to *FISCAM*, access controls limit access or detect inappropriate access to information resources and protect resources against unauthorized modification, loss, and disclosure. Access controls can be both logical and physical. Logical controls include user authentication, access to resources, and user permissions for actions. Physical controls restrict physical access to information resources and facilities.[22] Annual FISMA reports—including the fiscal year 2024 report—have repeatedly identified access controls as a nationwide issue for VA.[23] At the Lovell Federal Healthcare System, the OIG team evaluated selected NIST controls relevant to access control.[24] To evaluate this area, the team interviewed staff from OIT, facility management, and information system security and privacy; reviewed policies and procedures; conducted walk-throughs of the facility; and analyzed evidence. See appendix A for more information about the inspection's scope and methodology.

Finding 3: The Lovell Federal Healthcare System Had Five Access Control Deficiencies

The OIG team identified five deficiencies with access controls in the Lovell Federal Healthcare System.

Boundary Protection

The team found that not all networked medical devices or special-purpose systems were protected by restricting network access to the system. According to NIST, boundary protection can isolate parts of the network, such as system components that perform different mission or business functions. These boundaries limit unauthorized information flow among system components and can provide more protection for specific components.

Advances in medical technology and special-purpose systems have expanded the capability to store patient data and connect to healthcare networks. Consequently, these devices and systems pose potential risks for healthcare facilities. These risks include exposing such systems to malware and system integration challenges as well as losing sensitive patient data.

While VA criteria provide specific language for isolation of medical devices, they do not include language for isolating special-purpose systems. VA Directive 6550 provides requirements for medical devices, and VA Directive 6008 outlines isolation expectations for medical devices.[25] VA Directive 6008 mentions special-purpose systems but does not address the isolation of these

[22] GAO, *FISCAM*.

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

[24] NIST Special Publication 800-53.

[25] VA Directive 6550, *Pre-procurement Assessment and Implementation of Medical Devices/System,* June 3, 2019; VA Directive 6008, *Acquisition and Management of VA Information Technology Resources,* January 6, 2023.

systems across the VA network. Special-purpose systems share similar vulnerabilities to medical devices—vendor patch constraints, legacy operating systems, and operational criticality—all of which make isolation essential. Reinforcing specialized device isolation would align with VA Directive 6550, VA Handbook 6500, and boundary protection controls outlined in NIST's Risk Management Framework.

Management of Physical Facility Keys

The OIG 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. Separation of duties is a fundamental security principle for preventing unauthorized access.[26] 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.

Emergency Power Controls

During physical observations of the facility, the OIG team determined that communication closets did not meet federal and VA requirements for emergency power.[27] Based on a review of IT areas, the OIG found that:

- Several had uninterruptible power supply devices that needed to be serviced.
- Several had uninterruptible power supplies that were not plugged into power outlets identified as being connected to an emergency power supply; some had both of these issues.

An individual responsible for maintaining these devices told the OIG team that they were inundated with numerous critical and noncritical alerts, making it difficult to prioritize responses. Uninterruptible power supplies are electrical systems or mechanisms that provide emergency power when the main power source fails. They are typically used to protect devices and telecommunications equipment when an unexpected power outage could cause injuries, fatalities, business disruption, or loss of data. Uninterruptible power supplies differ from emergency power systems for backup generators because they provide near-instantaneous protection from interruptions. Without operational uninterruptible power supplies, equipment will not function during power fluctuations or outages, resulting in interruption of data flow and disruption of access to network resources.

[26] NIST Special Publication 800-53.

[27] NIST Special Publication 800-53; OIT, *Infrastructure Standard for Telecommunications Spaces*, ver. 3.1, July 2021.

In January 2026, the OIG team brought this finding to the facility's attention. In February 2026, the director of the healthcare system issued a memorandum where he acknowledged and formally accepted the minimal risk associated with the current uninterruptible power supply battery issues in the IT areas. Furthermore, this memorandum said that the uninterruptible power supply units were being monitored by facility staff and, while uninterruptible power supply servicing needs reduced the amount of time that backup power could be supplied, that was long enough to maintain the communications closets until emergency generator power was activated.

However, the team found that certain locations lacked appropriate emergency power coverage. The director's memorandum noted that there is a schedule to replace the uninterruptible power supplies.

Electrical Grounding

Of the IT areas reviewed by the OIG team, several did not meet federal and VA environmental security requirements related to the grounding of equipment.[28] Without proper grounding, 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.

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. According to VA Directive 6371, 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."[29] Additionally, 36 C.F.R. § 1226.24 requires a witness for the destruction of such documents.[30] A witness did not always observe the destruction of these documents at the Captain James A. Lovell Health Care Center. As a result, the healthcare system had no assurance that the paper records were appropriately destroyed. A compromise of these temporary paper records could result in financial and reputational loss to VA, which is entrusted to protect sensitive veteran data.

[28] NIST Special Publication 800-53; OIT, *Infrastructure Standard for Telecommunications Spaces*.

[29] VA Directive 6371, *Destruction of Temporary Paper Records*, April 8, 2014.

[30] 36 C.F.R. § 1226.24; "Disposition of Federal Records: A Records Management Handbook" (web page), National Archives and Records Administration, accessed February 3, 2026, https://www.archives.gov/files/records-mgmt/pdf/dfr-2000.pdf.

Finding 3 Conclusion

The OIG found that the Lovell Federal Healthcare System can improve access control deficiencies, including boundary protection, physical key management, emergency power, electrical grounding, and temporary records destruction. Inadequate access controls can result in unauthorized access to, modification of, or disclosure of sensitive data and programs and disruption of critical operations.

Recommendations 3–7

The OIG made the following recommendation to the assistant secretary for information, who also serves as chief information officer:[31]

3. Confirm appropriate network isolation and protections for all medical devices and special-purpose systems hosted on the Lovell Federal Healthcare System networks.

The OIG made the following recommendations to the director of the Lovell Federal Healthcare System, in collaboration with the assistant secretary for information and technology:

4. Separate the duties of maintaining physical blank key stock and making keys to improve physical access controls over key inventories.
5. Improve the process for monitoring and servicing uninterruptible power supplies that support the network infrastructure.
6. Complete the installation of grounding measures for all communications closets.
7. Establish a process to make sure a witness observes the destruction of temporary paper files that contain personally identifiable information and protected health information.

VA Management Comments

The VA Deputy Secretary, performing the delegable duties of the assistant secretary for information and technology and chief information officer, concurred with each recommendation. In response to recommendation 3, he said the healthcare system is strengthening security for medical devices and special-purpose systems by enhancing network segmentation and implementing additional protective controls appropriate to each system's operational requirements. For recommendation 4, the healthcare system fully implemented separation of duties and inventory controls for keys that includes limiting the individuals authorized to order blank keys; securing key stock; requiring a valid work order before issuing stock to the locksmith; and maintaining a continuously updated inventory to ensure visibility and

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

accountability. These controls satisfy the segregation of duties and accountability requirements OIG identified. For recommendation 5, he indicated the healthcare system is strengthening its monitoring and maintenance processes for uninterruptible power supplies that support critical network infrastructure.

For recommendation 6, the Deputy Secretary said the healthcare system is completing planned infrastructure improvements to equip all communications closets with appropriate grounding measures in accordance with applicable standards and organizational requirements. Finally, he said that to address recommendation 7, the healthcare system is strengthening its records handling and information protection procedures by enhancing controls over the destruction of temporary paper records containing sensitive information. The full text of the Deputy Secretary's response is included in appendix C.

OIG Response

Based on the evidence of corrective actions provided by VA in June 2026, the OIG considers recommendation 4 closed. The corrective action plans are responsive to the intent of the remaining recommendations. The OIG will monitor implementation of the remaining planned actions and will close recommendations 3, 5, 6, and 7 when VA provides evidence demonstrating it has addressed the identified issues.

Appendix A: Scope and Methodology

Scope

The VA Office of Inspector General (OIG) team conducted its work from January through June 2026. The team evaluated selected configuration management, security management, and access controls for VA information technology (IT) 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 IT security policies.[32] 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 OIG team examined relevant laws, guidance, and policies and prepared an inspection plan. The team visited the facility and inspected locations where IT resources are located. Additionally, the team interviewed Office of Information and Technology (OIT) staff, facility management staff, and information system security and privacy staff. The team conducted vulnerability and configuration scanning to determine local systems' security compliance. Finally, the team analyzed the results of the inspection, interviews, and scanning to identify control deficiencies and threats to security.

Internal Controls

Using the Government Accountability Office's *Standards for Internal Control in the Federal Government*, the OIG team assessed internal controls to determine whether they were significant to the inspection objective.[33] 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."[34] The OIG team identified internal control weaknesses during the inspection and proposed recommendations to address them.

---

[32] Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014); National Institute of Standards and Technology (NIST), Special Publication 800-53, revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020, updated December 10, 2020.

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

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

Data Reliability

The OIG team generated computer-processed data 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 team relied on the results of the scanning tools in identifying network device configuration. The team performed independent validation to supplement agency-provided information. The team completed data reliability checklists and internal process testing to ensure the data were reliable, sufficient, and appropriate to support the findings.

Government Standards

The OIG conducted this inspection in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.[35]

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

Appendix B: Background

Federal Information Security Modernization Act of 2014

The following are the stated goals of the Federal Information Security Modernization Act of 2014 (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 development and maintenance of minimum controls required to protect federal information and information systems.
- Provide a mechanism for improved oversight of federal agency information security programs.
- Acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions.
- Recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.[36]

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 provides oversight of the contractor's performance.[37]

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. NIST develops information security standards and guidelines in accordance

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

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

with its statutory responsibilities under FISMA. NIST Special Publication 800-53 provides a catalog of security and privacy controls for information systems and organizations.[38]

Federal Information System Controls Audit Manual

The Government Accountability Office developed the *Federal Information System Controls Audit Manual* (*FISCAM)* to assess information system controls. *FISCAM* groups information system controls of similar risk into six categories: business process controls, security management, access controls, segregation of duties, configuration management, and contingency planning. To help auditors evaluate information systems, *FISCAM* aligns control categories with NIST controls.[39]

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

[39] Government Accountability Office, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-24-107026, September 2024; NIST Special Publication 800-53.

Appendix C: VA Management Comments

Department of Veterans Affairs Memorandum

Date: July 17, 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, Inspection of Information Security at the Lovell Federal Healthcare System in Illinois, Project Number 2025-04267-AE-0168 (VIEWS 14915746)

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

1. Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) draft report, Inspection of Information Security at the Lovell Federal Healthcare System in Illinois (Project Number 2025-04267-AE-0168).

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

3. OIG made seven recommendations, and OIT concurs with all seven. Based on corrective action evidence OIT previously provided, OIG closed recommendations 1 and 4. OIT's written comments include a corrective action plan and target implementation date for the five remaining open recommendations.

The OIG removed point of contact information prior to publication.

(Original signed by)

Paul R. Lawrence, PhD

Attachments

Attachment

Office of Information and Technology
Action Plan
Office of Inspector General (OIG) Draft Report: Inspection of Information Security at the Lovell Federal Healthcare System in Illinois
(OIG Project Number 2025-04267-AE-0168)

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

Comment: Concur. The Department of Veterans Affairs (VA) Office of Information and Technology (OIT) concurs with the Office of Inspector General's (OIG) findings on vulnerability management. Captain James A. Lovell Federal Health Care System remediated or formally documented all identified vulnerabilities in a plan of action and milestone within the applicable VA policy timeframes in place at the time of the audit.

Based on corrective action evidence VA provided in June 2026, OIG closed this recommendation.

Recommendation 2: Improve 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.

Comment: Concur. Captain James A. Lovell Federal Health Care System is enhancing its baseline configuration management program to strengthen governance over network devices and database platforms. The facility is improving its monitoring and remediation processes to identify and address configuration deviations and vulnerabilities promptly, reducing cybersecurity risk and supporting compliance with applicable security requirements.

Recommendation 3: Ensure appropriate network isolation and protections for all medical devices and special-purpose systems hosted on the Lovell Federal Healthcare System networks.

Comment: Concur. Captain James A. Lovell Federal Health Care System is strengthening security for medical devices and special-purpose systems by enhancing network segmentation and implementing additional protective controls appropriate to each system's operational requirements. These corrective actions will reduce cybersecurity risk while preserving the availability, integrity, and safe operation of healthcare services.

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

Comment: Concur. Captain James A. Lovell Federal Health Care System fully implemented separation of duties and inventory controls for keys that includes limiting the individuals authorized to order blank keys; securing key stock; requiring a valid work order before issuing stock to the locksmith; and maintaining a continuously updated inventory to ensure visibility and accountability. These controls satisfy the segregation of duties and accountability requirements OIG identified.

Based on corrective action evidence VA provided in June 2026, OIG closed this recommendation.

Recommendation 5: Improve the process for monitoring and servicing uninterruptible power supplies that support the network infrastructure.

Comment: Concur. Captain James A. Lovell Federal Health Care System is strengthening its monitoring and maintenance processes for uninterruptible power supplies that support critical network infrastructure.

These improvements will increase infrastructure reliability and resilience, reduce the risk of service disruptions, and ensure the continued availability of critical network services.

Recommendation 6: Complete the installation of grounding measures for all communications closets.

Comment: Concur. Captain James A. Lovell Federal Health Care System is completing planned infrastructure improvements to equip all communications closets with appropriate grounding measures in accordance with applicable standards and organizational requirements. These efforts will improve reliability, resilience, and protection of critical communications equipment while reducing operational risk.

Recommendation 7: Establish a process to make sure a witness observes the destruction of temporary paper files that contain personally identifiable information and protected health information.

Comment: Concur. Captain James A. Lovell Federal Health Care System is strengthening its records handling and information protection procedures by enhancing controls over the destruction of temporary paper records containing sensitive information. These measures will reduce the risk of unauthorized disclosure, strengthening the facility's overall privacy and security posture.

The text of VA's management comments is reprinted verbatim as received from the department. 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	Allison Bennett Jodi Treszoks 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
Veterans Health Administration
Lovell Federal Healthcare System
VISN 3

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:
Illinois: Tammy Duckworth, Dick Durbin
Wisconsin: Tammy Baldwin, Ron Johnson
US House of Representatives:
Illinois: Mike Bost, Nikki Budzinski, Sean Casten, Danny K. Davis, Bill Foster, Jesús "Chuy" Garcia, Jonathan Jackson, Robin Kelly, Raja Krishnamoorthi, Darin LaHood, Mary Miller, Mike Quigley, Delia Ramirez, Jan Schakowsky, Brad Schneider, Eric Sorensen, Lauren Underwood
Wisconsin: Bryan Steil