US DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS HEALTH ADMINISTRATION

Inspection of Information Security at the VA Saginaw Healthcare System in Michigan

Information Security Inspection	**25-02113-77**	**May 28, 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 VA Saginaw Healthcare System in Michigan to assess compliance with federal cybersecurity standards under the Federal Information Security Modernization Act of 2014 (FISMA).[1] The inspection focused on three security control categories: configuration management, security management, and access controls. The OIG selected the VA Saginaw Healthcare System because it had not been previously visited as part of the annual FISMA audit. The OIG also notes that Saginaw transitioned to the new federal Electronic Health Record in April 2026.

The OIG visited the VA Saginaw Healthcare System in Michigan during the week of April 28, 2025. On April 30, the team alerted the Office of Information and Technology (OIT) to fire hazards in rooms that could affect information technology (IT) operations, and the healthcare system subsequently took action to eliminate the hazards. In July 2025, the OIG provided OIT 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 internal material is not being published by the OIG or distributed outside VA.

The OIG made 10 recommendations to improve configuration management, security management, and access controls to safeguard veterans' information.[2] As of February 2026, the healthcare system provided evidence that they addressed seven of the 10 recommendations related to findings concerning remediation of vulnerabilities, unscanned network segments, unapproved software, physical security deficiencies, protection of privileged accounts, verification of the identity of vendors and contractors, and protection of networked medical devices. Accordingly, recommendations 3 through 7, as well as 9 and 10, are considered closed. In March 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 10 recommendations.

What the Inspection Found

The team identified deficiencies related to configuration management, security management, and access controls during its inspection of the VA Saginaw Healthcare System. The healthcare system had five deficiencies in three configuration management controls. Facility staff did not consistently ensure that servers were configured correctly or that local databases were scanned

[1] Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. No. 113-283, § 3551.

[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 C.

for configuration compliance and vulnerabilities. Staff also did not ensure that all local area network segments were scanned for vulnerabilities, did not remediate all vulnerabilities within VA-defined time frames, and failed to create required action plans. Finally, staff were hosting unauthorized software on the network. Misconfigured systems and unmitigated vulnerabilities could compromise VA systems and place veterans' sensitive data at risk.

The healthcare system had one deficiency with security management. Although a physical security issue had been previously identified, OIT staff had not developed a plan of action to address it. Inadequate security management can prevent risk responses from aligning with VA's risk tolerance and enterprise risk management strategy and can result in insufficient protection of sensitive or critical information resources.

The healthcare system's access controls had five deficiencies, including the fire hazard discussed above. Facility staff had not implemented required controls for certain privileged accounts, and access to these accounts was not well controlled. Facility staff did not collect and review audit logs for local databases, did not consistently verify and document the identity of vendors or contractors before granting them access to information systems, and did not ensure all networked medical devices were protected by boundary segmentation of virtual local area networks. Inadequate access controls can result in unauthorized access to, modification of, or disclosure of sensitive data and programs, and disruption of critical operations.

Next Steps

The OIG will continue to 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.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

Contents

Abbreviations

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.[3] 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.[4] The FISMA audit is conducted in accordance with guidelines issued by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST).[5]

The 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 been assessed in the annual FISMA audit or had previously performed poorly.

The OIG conducted this inspection to determine whether the VA Saginaw Healthcare System in Michigan was meeting federal security guidance. The OIG selected the VA Saginaw Healthcare System because it had not been previously visited as part of the annual FISMA audit. The inspection team visited the Aleda E. Lutz VA Medical Center in Saginaw, Michigan, from April 28 through May 1, 2025. The OIG also notes that Saginaw transitioned to the new federal Electronic Health Record in April 2026.

In July 2025, the OIG provided the Office of Information and Technology (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 VA Saginaw Healthcare System, but other facilities across VA could benefit from reviewing this information and considering the OIG's recommendations.

---

[3] 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 rev. 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, September 2020, updated December 10, 2020.

[4] Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. No. 113-283, § 3551; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2024*, Report No. 24-01233-90, June 18, 2025.

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

Security Controls

NIST and OMB provide criteria for implementing security controls. NIST establishes security and privacy controls for systems to help organizations identify the controls needed to manage risk and to satisfy federal security and privacy requirements.[6] 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.[7]

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).[8] 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.[9]

This OIG information security inspection focused on three selected security control areas that are identified in the *Federal Information System Controls Audit Manual* (*FISCAM*), as shown in table 1. *FISCAM* groups related NIST security and privacy controls into categories that have similar types of risks. 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.[10]

[6] NIST, Special Publication 800-53 rev. 5.

[7] OMB Circular A-130.

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

[9] VA Handbook 6500.

[10] 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.*

OIT Structure and Responsibilities

The assistant secretary for information and technology serves as chief information officer and leads the OIT.[11] 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.[12] End user operations staff assigned to the VA Saginaw Healthcare System are responsible for managing system plans of action and milestones to ensure that all assessed and scanned vulnerabilities are documented.[13] The Cybersecurity Operations Center, part of the Office of Information Security, serves as the authoritative source for addressing and managing cybersecurity incidents.[14]

Results of Previous Projects

The OIG and Government Accountability Office (GAO) have previously reported VA's continued challenges with information security and protecting privacy and sensitive data.[15] These deficiencies could compromise the protection of VA data and information systems.

[11] VA Handbook 6500; VA, *VA Functional Organization Manual (FOM), vol. 2 of 2: Staff Offices*, ver. 8.1, 2023.

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

[13] 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.

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

[15] 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.

The VA Saginaw Healthcare System

The VA Saginaw Healthcare System provides healthcare services at 12 locations to more than 40,000 veterans living in 35 counties in the central and northern regions of Michigan's lower peninsula. Facilities include the Aleda E. Lutz VA Medical Center in Saginaw and 11 community-based outpatient clinics in Bad Axe, Cadillac, Clare, Traverse City, Gaylord, Grayling, Alpena, Oscoda, and Saginaw. The medical center and clinics have more than 1,500 employees who provide healthcare to over 40,000 veterans. The VA Saginaw Healthcare System's operations and workload costs are about $1.1 billion.[16]

[16] VA Saginaw Healthcare System, "Annual Report Fiscal Year 24, We Are Leading Change."

Results and Recommendations

The inspection team visited the Aleda E. Lutz VA Medical Center in Saginaw, Michigan, from April 28 through May 1, 2025. The team assessed configuration management, security management, and access controls and found that IT resources at the medical center overall are managed with care. For example, the main computer and telecommunication rooms were notably well organized and clean, and the team observed coordination and cooperation between OIT staff, facility management staff, privacy office staff, and VA police. However, the team found areas for improvement in all three control areas. The OIG made 10 recommendations to enhance OIT's processes and improve adherence to laws protecting veterans' information and VA data and information systems. The OIG will evaluate OIT's actions and will close the 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 the 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.[17] An effective configuration management process is essential to the security of information and systems.[18] At the VA Saginaw Healthcare System, the inspection team evaluated selected NIST controls relevant to configuration management.[19] To evaluate this control area, the team interviewed OIT staff, facility management staff, and information system security and privacy staff; reviewed local policies and procedures; conducted walk-throughs of the facility; assessed scan results from OIT; scanned local network devices for vulnerabilities and compliance; and analyzed evidence.[20]

Finding 1: The Healthcare System Had Five Configuration Management Deficiencies

The OIG team found five deficiencies within three configuration management controls at the VA Saginaw Healthcare System as described in the following sections.[21]

[17] GAO, *FISCAM*.

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

[19] NIST, Special Publication 800-53 rev. 5.

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

[21] NIST, Special Publication 800-53 rev. 5. For uniformity, the OIG uses the control name identified by NIST.

Baseline Configuration

Facility staff did not ensure that servers were compliant with configuration baselines. Additionally, facility staff did not ensure that all local databases were scanned quarterly for configuration compliance and for vulnerabilities.

Noncompliant Servers

The inspection team determined that VA Saginaw Healthcare System staff did not ensure that servers were compliant with baseline configurations. According to NIST, baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for system changes and include security and privacy control implementations. Maintaining baseline configurations requires creating new baselines as organizational systems change over time.[22]

To evaluate this control area, the team performed compliance scans to check the server configurations against their expected baselines. These scans identified multiple servers that deviated from VA-approved security baselines. For example, the scans identified security weaknesses related to access controls.

VA policy states that VA IT products will be configured in accordance with applicable Security Technical Implementation Guides that are developed by the Defense Information Systems Agency to provide general security compliance guidelines. Security Technical Implementation Guides are product-specific and document applicable federal policies and security requirements, as well as best practices and configuration guidelines.[23] VA standard operating procedure establishes that OIT area managers or designees will ensure all local systems comply with the VA baselines annually or as needed and will document deviations from the VA baselines.[24]

Servers were not compliant with VA-approved security baselines because the OIT area manager or information system owner did not request compliance scans on these servers and did not ensure that servers complied with Security Technical Implementation Guides.[25] Without compliance scans, facility staff will not be aware of configuration errors that could threaten the security of VA's sensitive data and information systems.

Having a configuration and change management process to protect against these risks is vital to the overall security posture of the organization. Configuration management is important because

[22] NIST, Special Publication 800-53 rev. 5.

[23] VA Handbook 6500.

[24] VA OIT, End User Services (EUS), *End User Operations (EUO), Security Controls-Configuration Management (CM), Standard Operating Procedure (SOP)*, ver. 1.1.1, March 18, 2025.

[25] OIT, in its End User Operations standard operating procedures, assigns roles and responsibilities equally to information system owners and area managers. However, area managers are not always the information system owner for all of the systems within their geographical area of operations.

as the complexity of information systems increases, the complexity of the processes used to create these systems also increases, as does the probability of accidental errors in configuration.[26] For VA, misconfigured systems can place veterans' sensitive data at risk of loss of confidentiality, integrity, or availability.

Unscanned Databases

The inspection team determined that VA Saginaw Healthcare System staff did not ensure that all local databases were scanned quarterly for configuration compliance and for vulnerabilities as required by policy. Several production databases lacked required periodic compliance and vulnerability scans. For the databases that had been scanned, there were multiple deviations from VA-approved security baselines, including misconfigurations related to account and password management.

The inspection team also determined that the healthcare system had not been scanning multiple databases for vulnerabilities on a quarterly basis. For the databases that had been scanned, there were multiple vulnerabilities. For example, VA scans identified security weaknesses related to improper access controls, misconfigurations, and patchable vulnerabilities.

VA policy requires scans of databases hosted in the production environment. VA policy also specifies that database scanning shall be performed at least quarterly to maintain an authorization to operate. The VA Cybersecurity Operations Center conducts quarterly database vulnerability scans as requested by information system owners or system stewards.[27] However, some VA Saginaw Healthcare System databases were not being scanned for compliance or vulnerabilities because the OIT area manager or information system owner had not been requesting these quarterly scans.

According to Microsoft, databases may contain some of any organization's most sensitive data, which makes these data an obvious target for attackers to sell, encrypt, or destroy. Furthermore, databases have an extensive attack surface and are often misconfigured, which can lead to an attacker gaining access.[28] VA's policy explains that misconfiguration of databases can include configuration mistakes, identification and access control issues, missing patches, or any

[26] Carnegie Mellon University, *CRR (Cyber Resilience Review) Supplemental Resource Guide, vol. 3, Configuration and Change Management*, ver. 1.1, 2016.

[27] VA OIT, Infrastructure Operations, *Information System Vulnerability Management Plan*, ver. 2.0, April 22, 2024. NIST defines the production environment as an environment where functionality and availability must be ensured for the completion of day-to-day activities.

[28] "Microsoft Defender for Cloud Blog" (website), Microsoft, accessed April 1, 2025, https://techcommunity.microsoft.com/blog/microsoftdefendercloudblog/microsoft-defender-for-cloud---sql-servers-on-machines-should-have-vulnerability/3879850.

combination of settings that could lead to escalation of privileges attacks, data leakage, denial-of-service, or unauthorized modification of data held within data stores.[29]

Vulnerability Monitoring and Scanning

Facility staff did not remediate all vulnerabilities within required time frames and did not document mitigating controls using plans of action and milestones. Additionally, facility staff did not ensure all the facility's local area network segments were scanned for vulnerabilities.

Untimely Remediation of Vulnerabilities

According to NIST, new vulnerabilities are regularly discovered due to the complexity of modern software, systems, and other factors. It is important that these vulnerabilities are added to the list of vulnerabilities to be scanned to ensure that the organization can take mitigation steps in a timely manner.[30]

The inspection team's scans found multiple vulnerabilities past their remediation date on devices that had not been identified in VA's vulnerability reports in the Information Central Analytics and Metrics Platform.[31] Facility staff had not created plans of action and milestones documents in VA's governance, risk, and compliance tool for the high vulnerability as required.[32]

Additionally, the OIG team determined that the healthcare system hosted high and critical known exploitable vulnerabilities that had not been remediated within VA-defined timelines. These vulnerabilities are cataloged by the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security.[33]

NIST recommends performing periodic vulnerability assessments that include employing monitoring tools and remediating legitimate vulnerabilities, and *FISCAM* emphasizes that vulnerability scan reports and results from monitoring inform the entity's risk assessment process.[34] VA's Cybersecurity Operations Center performs monthly vulnerability scans, and information system owners, the area manager, or system stewards are required to address

---

[29] VA OIT, Infrastructure Operations, *Information System Vulnerability Management Plan*.

[30] NIST, Special Publication 800-53 rev. 5; VA OIT, Development, Security, and Operations, *Information System Vulnerability Management Plan*, ver. 1.0, March 28, 2022.

[31] VA OIT, *Information Central Analytics and Metrics Platform (ICAMP) User Guide*, February 2023. ICAMP is a tool for organizing security and operational data sources across the enterprise. It centralizes reporting and metrics for operational processes, technologies, and services.

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

[33] Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, *Known Exploited Vulnerabilities Catalog*, accessed March 28, 2025, https://www.cisa.gov/known-exploited-vulnerabilities-catalog. The agency explains that these vulnerabilities have been exploited, and organizations should use the catalog as an input for their vulnerability management prioritization.

[34] NIST, Special Publication 800-53 rev. 5; GAO, *FISCAM*.

vulnerabilities, either through timely remediation or by documented mitigation in a plan of action and milestones.[35] VA requires that findings identified in technical scans should be mitigated from the initial detection date within specified remediation time frames.[36]

VA Saginaw Healthcare System staff had remediated or created plans of action and milestones for most vulnerabilities within VA-defined time frames. However, the existence of a high vulnerability past its remediation date and without a plan of action and milestones indicates that improved vulnerability tracking is needed. According to Carnegie Mellon University, vulnerability management is a key component in planning for and determining the appropriate implementation of controls and the management of risk. Vulnerability management ensures that the organization understands its weaknesses so that it can plan accordingly.[37]

Unmitigated vulnerabilities could compromise VA systems, which can include veterans' sensitive personal information. If VA does not mitigate vulnerabilities within VA-defined time frames, this may result in harm to individuals whose information is improperly accessed and disclosed, and the department may face legal liability, remediation costs, and a loss of public trust.[38] In January 2026, the healthcare system provided evidence that they had remediated vulnerabilities, including known exploitable vulnerabilities, or had assigned action plans to address remaining vulnerabilities.

Unscanned Network Segments

The inspection team determined that the VA Cybersecurity Operations Center was not scanning all the VA Saginaw Healthcare System's local area network segments. The OIG team found that some local area network segments had not been scanned for vulnerabilities.

OIT area managers and information system owners are responsible for managing system plans of action and milestones to ensure that they document all assessed and scanned vulnerabilities and are responsible for monitoring the Information Central Analytics and Metrics Platform to maintain awareness of the system's information security posture. Therefore, area managers and information system owners are expected to review monthly scans and to verify that scanning provides accurate coverage.[39]

---

[35] VA OIT, End User Services (EUS), *End User Operations (EUO), Security Controls-Risk Assessment (RA), Standard Operating Procedure (SOP)*. VA uses the terms "system steward," "information system owner," and "area manager" interchangeably in several End User Operations standard operating procedures.

[36] VA OIT, *Authorization Requirements Standard Operating Procedures*, version 1.64, June 12, 2024.

[37] Carnegie Mellon University, *CRR (Cyber Resilience Review) Supplemental Resource Guide, vol. 4, Vulnerability Management*, ver. 1.1, 2016.

[38] NIST, Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010.

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

Not all of the healthcare system's local area network segments were being scanned monthly because the OIT area manager was not validating the results of the monthly Cybersecurity Operations Center scans or informing the center of corrections needed. If vulnerability scans do not provide accurate coverage, the organization will not have an accurate assessment of its risk posture. This situation can prevent an organization from taking required actions such as remediating vulnerabilities.[40] In February 2026, the healthcare system provided evidence that they had remediated the finding by validating scan results and decommissioning unneeded network segments.

Software, Firmware, and Information Integrity

VA Saginaw Healthcare System staff hosted unapproved software on the network without seeking authorization and without having corresponding plans of action and milestones to define constraints and compensating controls. According to *FISCAM*, unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Also, unapproved software applications may be inadvertently installed when an otherwise authorized application is downloaded or patched.[41]

VA OIT's Enterprise Endpoint Management and Reporting site provides an internal online report on unapproved software. On this site, the team observed multiple installations of many unapproved applications. The VA Technical Reference Model directs all OIT staff and contractors to use the internal website to ensure all technologies, programs, and projects comply with a single model. The Technical Reference Model clarifies that unapproved software can be "Authorized with Constraints (Plan of Action & Milestones)." This means the technology or standards can be used only if a VA plan of actions and milestones review is conducted and signed.[42] VA policy requires that system owners prepare plans of actions and milestones if there is a valid business reason for ongoing use of the software.

While the OIT area manager provided evidence of being actively involved in the process for removal of unapproved software, this software remained on the network without OIT staff having sought authorization and without documenting corresponding plans of action and milestones to define constraints and compensating controls.

VA states that adherence to the Technical Reference Model is essential to improving and controlling the technical environment in VA, optimizing performance, and minimizing conflicts that adversely affect development and usability. Unauthorized software installations on VA

---

[40] Carnegie Mellon University, *CRR (Cyber Resilience Review) Supplemental Resource Guide, vol. 4, Vulnerability Management*.

[41] "Unwanted software" (website), Microsoft, accessed July 8, 2025, https://learn.microsoft.com/en-us/defender-endpoint/malware/unwanted-software; "Software Principles" (website), Google, accessed July 8, 2025, https://www.google.com/about/software-principles.html.

[42] "VA Technical Reference Model v 25.5" (website), VA OIT. (This website is not publicly accessible.)

systems both violate VA policy and put the enterprise at risk.[43] To remediate systems with unauthorized software, the software must be removed or replaced with an approved version.[44] Prior to publication of this report, the healthcare system provided evidence that they had removed unapproved software or had assigned action plans to address remaining software.

Finding 1 Conclusion

VA Saginaw Healthcare System staff can improve configuration management controls. Specifically, the OIG team identified deficiencies with certain NIST security and privacy controls, including baseline configuration; vulnerability monitoring and scanning; and software, firmware, and information integrity. Annual FISMA reports have repeatedly identified configuration management as a nationwide issue for VA.[45]

Recommendations 1–5

The OIG made five recommendations to the assistant secretary for information and technology, who also serves as chief information officer:[46]

1. Remediate servers that are not compliant with configuration standards and ensure periodic compliance scanning of servers.
2. Remediate databases that are not compliant with configuration standards and ensure quarterly compliance and vulnerability scanning of databases.
3. Remediate vulnerabilities within VA-defined time frames and document mitigations for vulnerabilities that cannot be remediated on time.
4. Comprehensively scan all the facility's local area network segments for vulnerabilities.
5. Prepare plans of action and milestones for unapproved software still in use.

In response to the OIG's inspection, VA took corrective actions and provided documentation of those actions in January and February 2026; therefore, the OIG considers recommendations 3, 4, and 5 closed.

[43] "VA Technical Reference Model v 25.5" (website), VA OIT.

[44] "Introduction to Unauthorized Software" (website), VA OIT. (This website is not publicly accessible.)

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

[46] 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.

VA Management Comments

The Deputy Secretary of VA, performing the delegable duties of the assistant secretary for information and technology and chief information officer, concurred with all five recommendations in this finding. Appendix C includes the full text of the comments.

To address recommendation 1, the Deputy Secretary stated that local OIT staff will review quarterly server scan reports and remediate any discrepancies to comply with configuration standards. For recommendation 2, he said local OIT staff will review quarterly database scan reports and remediate any discrepancies to comply with configuration standards.

OIG Response

The Deputy Secretary provided acceptable action plans for open recommendations 1 and 2. The OIG will continue to evaluate OIT's actions and will close these 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.

II. Security Management Controls

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.[47] The inspection team evaluated applicable policies and procedures and risk response. To evaluate this control area, the team 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.[48]

Finding 2: The Healthcare System Had One Security Management Deficiency

The inspection team identified one deficiency with security management at the VA Saginaw Healthcare System. Facility staff did not develop a plan of action and milestones document to address a physical security deficiency, and this resulted in a weakness in the NIST control, "Risk Response." Risk Response describes how an organization responds to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.[49]

Risk Response

The inspection team found that OIT personnel at the VA Saginaw Healthcare System did not develop a plan of action and milestones document for a physical security deficiency that affected IT operations, as required. VA police at the healthcare system had identified the deficiency and the facility had a plan to address it. However, OIT personnel had not separately documented the risk and did not develop a plan of action and milestones document in their governance, risk, and compliance tool.

VA's directive for cybersecurity states that plans of action and milestones are implemented to ensure that security and privacy programs and associated systems are developed and maintained, and that these plans document the actions facilities take to manage risk and address deficiencies. The directive explains that VA manages risk through strengthening existing controls or implementing new controls, accepting the risk with appropriate justification or rationale, sharing or transferring the risk, or rejecting the risk. If VA mitigates the risk and the mitigation cannot be completed immediately, a plan of action and milestones should be generated.[50] VA policy also specifies that information system owners and information system security officers will document

[47] GAO, *FISCAM*.

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

[49] NIST, Special Publication 800-53 rev. 5.

[50] VA Directive 6500.

vulnerabilities that cannot be remediated within an established time frame in a plan of action and milestones.[51]

A plan of action and milestones was not prepared for this deficiency because the OIT area manager and information system security officer believed a related physical security improvement had addressed the deficiency. Based on documentation provided by facility management personnel, the inspection team determined that the improvement addressed a separate requirement. Without documenting the plan to address this deficiency, the risk is not communicated to senior OIT management, and senior management cannot make risk-informed decisions and ensure that vulnerability management practices align with VA's risk tolerance and enterprise risk management strategy.[52] This can result in insufficient protection of sensitive or critical information resources.[53] In January 2026, the healthcare system provided evidence that they had corrected the physical security deficiency and that it had passed inspection by the local VA police.

Finding 2 Conclusion

VA Saginaw Healthcare System staff can improve their response to risk. Specifically, the OIG team identified a deficiency with risk response related to a physical security deficiency. The fiscal year 2024 FISMA report identified continuing deficiencies related to VA's security management controls.[54]

Recommendation 6

The OIG made one recommendation to the assistant secretary for information and technology, who also serves as chief information officer:[55]

6. Remediate or document mitigations for physical security deficiencies that can affect information technology operations and resources.

In response to the OIG's inspection findings, VA took corrective action and provided documentation in January 2026; therefore, the OIG considers this recommendation closed. That said, the Deputy Secretary of VA, performing the delegable duties of the assistant secretary for information and technology and chief information officer, concurred with recommendation 6.

[51] VA OIT, Infrastructure Operations, *Information System Vulnerability Management Plan*.

[52] VA OIT, Infrastructure Operations, *Information System Vulnerability Management Plan.*

[53] GAO, *FISCAM*.

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

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

III. Access Controls

According to *FISCAM*, access controls limit access or detect inappropriate access to information resources and protect resources against unauthorized modification, loss, and disclosure. Access controls address logical and physical access. Logical controls include user authentication, access to resources, and user permissions for actions. Physical controls restrict physical access to information resources and facilities.[56] Annual FISMA reports have repeatedly identified access controls as a nationwide issue for VA.[57] At the VA Saginaw Healthcare System, the inspection team evaluated selected NIST controls relevant to access control.[58] To evaluate this control 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.[59]

Finding 3: The Healthcare System Had Five Access Control Deficiencies

The inspection team identified five deficiencies with access controls in the VA Saginaw Healthcare System as described below.

Least Privilege

The inspection team found that VA Saginaw Healthcare System staff did not enforce "least privilege" for certain privileged accounts or sufficiently restrict access to these accounts. According to NIST, the principle of least privilege is to allow only authorized access for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.[60] OIT also requires enforcement of least privilege, allowing only authorized access necessary to accomplish assigned tasks.[61]

VA policy requires that certain privileged accounts have an identified custodian who will be responsible for their proper use. Accounts requiring elevated privileges should be requested using VA privileged access workflow approval processes, and account custodians should ensure that passwords are only known by delegates directly supporting the account.[62]

---

[56] GAO, *FISCAM*.

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

[58] NIST, Special Publication 800-53 rev. 5.

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

[60] NIST, Special Publication 800-53 rev. 5.

[61] VA OIT, End User Services (EUS), *End User Operations (EUO) Security Controls-Access Control (AC), Standard Operating Procedure (SOP)*, March 8, 2023.

[62] VA OIT, *Enterprise Active Directory User Account Management Standard Operating Procedure*, January 2025.

According to the OIT area manager, the healthcare system had not implemented required controls on certain privileged accounts due to the additional cost of enabling it. The healthcare system had a plan of action and milestones recommending working with vendors to bring systems into compliance. Access to certain privileged account usernames and passwords was not sufficiently controlled—all local OIT staff had access to the information without any accountability to record when specific staff members used the accounts. The area manager explained that this was due to the small number of OIT staff. The area manager should consider further restricting this access to individual custodians directly responsible for using the accounts and implementing some control to maintain a record of accountability.

Using privileged accounts without required controls is a risk because according to the General Services Administration, these types of accounts are most likely to be targeted by cybercriminals or abused by malicious insiders. The General Services Administration adds that unwanted behavior or compromised privileged accounts are responsible for the most high-profile federal and private security breaches.[63] In January 2026, the healthcare system provided evidence that they took action to secure the privileged accounts.

Audit Record Review, Analysis, and Reporting

The inspection team found that VA Saginaw Healthcare System staff were not regularly reviewing audit logs for privileged users on local databases. According to NIST, audit record review, analysis, and reporting cover information security and privacy-related logs. Audit logs collect system events significant and relevant to the security of systems and the privacy of individuals. These logs also support specific monitoring and auditing needs. Event types include password changes, failed log-ons or failed access to systems, security or privacy attribute changes, administrative privilege usage, personal identity verification credential usage, data action changes, query parameters, or external credential usage.[64]

VA requires that system audit data are collected, reviewed, and analyzed for indication of inappropriate or unusual activity and for reporting to law enforcement or other investigating agencies.[65] OIT's standard operating procedure for audit and accountability assigns the responsibility for managing auditing for any local systems not managed by the enterprise to the area manager or information system owner. Among the defined audit events, the procedure

[63] General Services Administration, *Privileged Identity Playbook*, ver. 1.2, December 29, 2022.

[64] NIST, Special Publication 800-53 rev. 5.

[65] VA, Directive 6500; Handbook 6510, *VA Identity, Credential, and Access Management*, September 27, 2024; VA OIT, End User Services (EUS), *End User Operations (EUO), Security Controls-Audit and Accountability (AU)), Standard Operating Procedure (SOP)*, ver. 1.1.1, March 8, 2023.

emphasizes an overall responsibility to report any indication of inappropriate or unusual activity and any activity that can present a risk to the security of the information system.[66]

Because administering databases requires privileged accounts and the use of administrative privileges is an auditable event, database audit logs should be reviewed regularly. Operating systems and security software provide the foundation and protection for applications, which are used to store, access, and manipulate the data used for the organization's business processes.[67] Application logs are particularly valuable for application-related security incidents, auditing, and compliance efforts.

OIT's standard operating procedure for audit and accountability does not assign an interval for review of database audit logs. The procedure does identify vulnerability reports as audit events to be reviewed monthly. OIT's Threat Assessment and Analysis Portal states that nondatabase assets are scanned for vulnerabilities monthly and databases quarterly.[68] VA should clearly define intervals for reviewing database audit logs and vulnerability scan results.

The healthcare system was not regularly collecting and reviewing audit logs for local databases because the OIT area manager or information system owners had not established a process to ensure that this is done. The area manager explained that the facility does not have any database administrators on-site and has only one technician who manages the installation of a certain type of database software.

According to NIST, routine log reviews and analysis help identify security incidents, policy violations, fraudulent activity, and operational problems shortly after they have occurred and provide useful information for resolving such problems. Logs can also facilitate auditing and forensic analysis, support the organization's internal investigations, help establish baselines, and identify operational trends and long-term problems.[69] Without logs, the facility may have limited evidence to support investigation of a security incident.[70] Breaches involving personally identifiable information can harm individuals and organizations due to identity theft, embarrassment, or blackmail, and organizational harms may include a loss of public trust, legal liability, or remediation costs.[71]

---

[66] VA OIT, End User Services (EUS), *End User Operations (EUO), Security Controls-Audit and Accountability (AU), Standard Operating Procedure (SOP)*.

[67] NIST, Special Publication 800-92, *Guide to Computer Security Log Management*, September 2006.

[68] "Threat Assessment and Analysis Portal, Vulnerability Scanning Services" (website), VA OIT. (This website is not publicly accessible.)

[69] NIST, Special Publication 800-92.

[70] VA Handbook 6500.2, *Management of Breaches Involving Sensitive Personal Information*, June 30, 2023.

[71] NIST, Special Publication 800-122.

Physical Access Control

The inspection team found that OIT personnel at the VA Saginaw Healthcare System did not consistently verify and document the identity of vendors or contractors before granting them access to IT resources. The facility did not consistently record required information when performing vendor and contractor identification checks. Documentation of non-employee identity verification was inconsistent.

Physical access controls limit access or detect inappropriate access to information resources, thereby protecting these resources against unauthorized modification, loss, and disclosure.[72] Such controls may include physical access control logs or records, guards, or physical access devices and barriers to prevent movement from publicly accessible areas to nonpublic areas. Physical access devices may include items such as keys, locks, card readers, and cameras.[73]

OIT's standard operating procedure for physical and environmental security controls requires authorized individuals to verify the identity of vendors or contractors before access is granted.[74] It also requires the area manager or their designee to review physical access logs quarterly or after a security violation or incident. The inspection team found that the area manager did review access logs quarterly.

OIT staff at the VA Saginaw Healthcare System did not consistently verify and record required information when performing vendor and contractor identification checks because the OIT area manager had not reinforced the need to meet this requirement.

Physical security programs and controls protect IT resources from damage, loss, theft, or unauthorized physical access. If VA cannot implement controls to adequately protect IT resources and the sensitive data VA processes—including from misuse by insiders, vendors, and contractors—individuals whose information is improperly accessed and disclosed may be harmed, and the department may face legal liability, remediation costs, and a loss of public trust.[75] In October 2025, the healthcare system provided evidence that they took corrective action and are consistently documenting the identity of vendors or contractors.

Fire Protection

On April 30, the inspection team notified VA Saginaw Healthcare System OIT staff about unsealed spaces and conduits in rooms that could affect IT operations—issues that were later confirmed to be previously unknown to them. Unsealed spaces increase the risk that fire and

[72] GAO, *FISCAM*.

[73] NIST, Special Publication 800-53 rev. 5.

[74] VA OIT, End User Services (EUS), *End User Operations (EUO), Security Controls-Physical and Environmental Security (PE), Standard Operating Procedure*, version 1.0.4, March 18, 2025.

[75] NIST, Special Publication 800-122; VA Directive 6500.

smoke could spread. According to NIST, the provisions of fire detection and suppression systems apply primarily to facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms.[76] If VA cannot implement controls to adequately protect VA IT resources and the sensitive data VA processes, it may not be able to limit or mitigate a potential cybersecurity and privacy event. In July 2025, following the inspection team's site visit, the healthcare system provided evidence that the unsealed spaces had been fixed. Therefore, the OIG considers the security deficiency resolved.

Boundary Protection

The inspection team found that not all networked medical devices in the VA Saginaw Healthcare System were protected by boundary segmentation of the virtual local area networks they reside on. 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.[77]

Advances in medical technology have expanded the capability to store patient data and connect to healthcare networks. Network-connected medical technology poses potential risks for healthcare facilities, such as increased bandwidth competition on the VA network, increased risk for exposure to malware, system integration challenges, increased data storage requirements, and increased chance of loss of sensitive patient data.[78]

VA policy states that with very limited exceptions, all network-connected medical devices shall be isolated on a medical device isolation architecture virtual local area network and defines "medical device isolation architecture" as a standard process that uses a protected virtual local area network structure to isolate and secure networked medical devices with an access control list.[79]

Not all networked medical devices in the VA Saginaw Healthcare System were protected as required because the Office of Information Security Specialized Device Cybersecurity

[76] NIST, Special Publication 800-53 rev. 5. VA standards for telecommunications spaces require that air penetrations are sealed to maintain fire and smoke barriers and to minimize cooling air pressure loss; VA OIT, *Infrastructure Standard for Telecommunications Spaces (ISTS)*, ver. 4.0, June 1, 2023. VA's Fire Protection Design Manual specifies that fire and smoke barriers must be provided as required by the National Fire Protection Association 101, Life Safety Code; VA, *Fire Protection Design Manual*, Ninth Edition, November 1, 2023. The National Fire Protection Association explains that managing the spread of fire through the construction of barriers designed to limit the transfer of heat, smoke, and, in some cases, both, is achieved by compartmentation; National Fire Protection Association, 101, *Life Safety Code*, 2024.

[77] NIST, Special Publication 800-53 rev. 5.

[78] VA Directive 6550, *Pre-Procurement Assessment and Implementation of Medical Devices/Systems*, June 3, 2019.

[79] VA Directive 6550; VA Directive 6008, *Acquisition and Management of VA Information Technology Resources,* January 6, 2023.

Department had not ensured that these devices were protected by access control lists for the virtual local area networks they reside on.[80] In February 2026, the healthcare system provided evidence of their remediation efforts by decommissioning unneeded virtual local area networks, adding access control lists where needed, and identifying virtual local area networks that did not require access control lists due to other protections in place.

Finding 3 Conclusion

The inspection team found that the VA Saginaw Healthcare System can improve access control deficiencies with NIST security and privacy controls, including least privilege; audit record review, analysis, and reporting; physical access control; and boundary protection. Inadequate access controls can result in unauthorized access to, modification of, or disclosure of sensitive data and programs, and disruption of critical operations.

Recommendations 7–10

The OIG made four recommendations to the assistant secretary for information and technology, who also serves as chief information officer:[81]

7. Implement required controls on certain privileged accounts and ensure limited access to these accounts.
8. Define intervals for review of database audit logs and vulnerability scan results and ensure regular collection and review of database audit logs in accordance with policy.
9. Verify and document the identity of vendors or contractors consistently before granting them access to information technology resources.
10. Provide boundary protection for all networked medical devices hosted on the VA Saginaw Healthcare System virtual local area networks.

In response to the OIG's findings, VA took corrective actions and provided documentation during the inspection; therefore, the OIG considers recommendations 7, 9, and 10 closed.

[80] VA OIT, Office of Information Security (OIS), Information Security Policy and Strategy (ISPS), Specialized Device Cybersecurity Department (SDCD), *Enterprise Risk Analysis Process for Specialized Devices/Systems (SD/S) User Guide*, ver. 5.1, March 4, 2024.

[81] 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.

VA Management Comments

The Deputy Secretary of VA, performing the delegable duties of the assistant secretary for information and technology and chief information officer, concurred with recommendations 7 through 10. Appendix C includes the full text of the comments.

To address recommendation 8, the Deputy Secretary stated that local OIT staff are conducting all policy-based audit review requirements and documenting any findings. He noted that OIT is monitoring implementation activities to validate effectiveness.

OIG Response

The Deputy Secretary provided an acceptable action plan to address recommendation 8. The OIG will continue to evaluate OIT's actions and will close this recommendation once OIT provides complete documentation and sufficient evidence that it has addressed the intent of the recommendation and the issues identified in this report.

Appendix A: Background

Federal Information Security Modernization Act of 2014 (FISMA)

The following are the stated goals of FISMA:

- Provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.
- Recognize the highly networked nature of the current federal computing environment and provide effective government-wide management and oversight of the related information security risks.
- Provide for the development and maintenance of 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.[82]

FISMA also requires an annual 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.[83]

National Institute of Standards and Technology (NIST) Information Security Guidelines

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 with its statutory responsibilities under the FISMA of

[82] Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. No. 113-283, § 3551.

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

2014. NIST Special Publication 800-53 provides a catalog of security and privacy controls for information systems and organizations.[84]

Federal Information System Controls Audit Manual (*FISCAM*)

The Government Accountability Office (GAO) developed *FISCAM*, a methodology for assessing 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.[85]

[84] NIST, Special Publication 800-53 rev. 5*, Security and Privacy Controls for Federal Information Systems and Organizations*, September 2020, updated December 10, 2020.

[85] Government Accountability Office (GAO), *Federal Information System Controls Audit Manual (FISCAM)*, GAO-24-107026, September 2024; NIST Special Publication 800-53 rev. 5.

Appendix B: Scope and Methodology

Scope

The inspection team conducted its work from April 2025 through February 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 of 2014 (FISMA), National Institute of Standards and Technology (NIST) security guidelines, and VA's IT security policies. 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, 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 (GAO) *Standards for Internal Control in the Federal Government*, the VA Office of Inspector General (OIG) team assessed internal controls to determine whether they were significant to the inspection objective.[86] 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.[87] The OIG team identified internal control weaknesses during the inspection and proposed recommendations to address them.

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

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

Data Reliability

The inspection team generated computer processed data by using network scanning tools. The results of the scans were provided to OIT. The team used industry standard information system security tools to identify information systems on the VA network and to capture relevant configuration information, which is used to identify vulnerabilities and determine 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 tools in identifying network device configuration. The team performed its own scans to supplement the agency's scans. The team completed data reliability checklists and internal process testing to ensure that the data were reliable, sufficient, and appropriate to support the findings.

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*.[88]

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

Appendix C: VA Management Comments

Department of Veterans Affairs Memorandum

Date: March 20, 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 VA Saginaw Healthcare System in Michigan (VIEWS 14412111)

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 Saginaw Healthcare System in Michigan* (Project Number 2025-02113-AE-0085). The Office of Information and Technology (OIT) concurs with OIG's recommendations and submits the attached written comments.

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 ten recommendations, of which OIT concurs with all ten. Based on the evidence of corrective actions previously provided by OIT, OIG considers recommendations 3-7 and 9-10 to be closed. OIT is providing a corrective action plan and target implementation date for the remaining three open recommendations.

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 Saginaw Healthcare System in Michigan
Project Number 2025-02113-AE-0085

Recommendation 1: Remediate servers that are not compliant with configuration standards and ensure periodic compliance scanning of servers.

Comments: Concur. The Department of Veterans Affairs (VA) Office of Information and Technology (OIT) concurs with the Office of Inspector General's (OIG) recommendation. Local OIT staff will review quarterly server scan reports and remediate any discrepancies in compliance with configuration standards.

Expected Completion Date: June 30, 2026.

Recommendation 2: Remediate databases that are not compliant with configuration standards and ensure quarterly compliance and vulnerability scanning of databases.

Comments: Concur. Local OIT staff will review quarterly database scan reports and remediate any discrepancies in compliance with configuration standards.

Expected Completion Date: June 30, 2026.

Recommendation 3: Remediate vulnerabilities within VA-defined timeframes and document mitigations for vulnerabilities that cannot be remediated on time (closed).

Comments: Concur. OIT remediated all identified vulnerabilities or documented action plans in a plan of action and milestone.

Expected Completion Date: Completed, January 27, 2026.

Based on the evidence of corrective actions previously provided by OIT, the Office of the Inspector General (OIG) agreed to close recommendation 3.

Recommendation 4: Comprehensively scan all the facility's local area network segments for vulnerabilities (closed).

Comments: Concur. OIT ensured that virtual local area networks are appropriately configured and are subject to regular scanning by the designated scan teams.

Expected Completion Date: Completed, February 3, 2026.

Based on the evidence of corrective actions previously provided by OIT, OIG agreed to close recommendation 4.

Recommendation 5: Prepare plans of action and milestones for unapproved software still in use (closed).

Comments: Concur. OIT created plans of action and milestones to document all unapproved software which is still in use.

Expected Completion Date: Completed, February 6, 2026.

Based on the evidence of corrective actions previously provided by OIT, OIG agreed to close recommendation 5.

Recommendation 6: Remediate or document mitigations for physical security deficiencies that can affect IT operations and resources (closed).

Comments: Concur. The facility remediated the physical security deficiency and confirmed that it had passed inspection by the local VA police.

Expected Completion Date: Completed, January 12, 2026.

Based on the evidence of corrective actions previously provided by OIT, OIG agreed to close recommendation 6.

Recommendation 7: Implement required controls on certain privileged accounts and ensure limited access to these account usernames and passwords (closed).

Comments: Concur. Local OIT acted to secure the privileged accounts through implementation of required controls and ensuring limited access to account usernames and passwords.

Expected Completion Date: Completed, January 28, 2026.

Based on the evidence of corrective actions previously provided by OIT, OIG agreed to close recommendation 7.

Recommendation 8: Define intervals for review of database audit logs and vulnerability scan results and ensure regular collection and review of database audit logs in accordance with policy.

Comments: Concur. Local OIT is conducting all policy-based audit review requirements and documenting any findings. OIT is monitoring implementation activities to validate effectiveness.

Expected Completion Date: June 30, 2026.

Recommendation 9: Verify and document the identity of vendors or contractors consistently before granting them access to IT resources (closed).

Comments: Concur. The facility implemented requirements for verifying the identity of visitors and non-employees prior to granting them physical access to information technology resources.

Expected Completion Date: Completed, November 7, 2025.

Based on the evidence of corrective actions previously provided by OIT, OIG agreed to close recommendation 9.

Recommendation 10: Provide access control list protection for all networked medical devices hosted on the VA Saginaw Healthcare System virtual local area networks (closed).

Comments: Concur. OIT implemented access control lists on all networked medical devices hosted on the VA Saginaw Healthcare System's virtual local area networks.

Expected Completion Date: Completed, February 3, 2026.

Based on the evidence of corrective actions previously provided by OIT, OIG agreed to close recommendation 10.

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 George Ibarra Tim Moorehead Justin Skeen
Other Contributors	Jill Russell Rashiya Washington

Report Distribution

VA Distribution

Office of the Secretary
Office of Accountability and Whistleblower Protection
Office of Congressional and Legislative Affairs
Office of General Counsel
Office of Information and Technology
Office of Public and Intergovernmental Affairs
VISN 10: VA Healthcare System
Aleda E. Lutz VA Medical Center

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: Gary Peters, Elissa Slotkin
US House of Representatives: Jack Bergman, Lisa McClain, Kristen McDonald Rivet, John Moolenaar