US DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS HEALTH ADMINISTRATION

Inspection of Information Security at the Battle Creek Healthcare System in Michigan

Information Security Inspection	**24-02575-50**	**May 1, 2025**

BE A
VOICE FOR
VETERANS
REPORT WRONGDOING
vaoig.gov/hotline | 800.488.8244

OUR MISSION

To serve veterans and the public by conducting meaningful independent oversight of the Department of Veterans Affairs.

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

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

The fiscal year (FY) 2023 FISMA audit report indicated that VA continues to face significant challenges meeting the law's requirements. All the report's 25 recommendations made to VA were repeated from the prior year; they included addressing deficiencies in configuration management, contingency planning, security management, and access controls.[2] Appendix A details these recommendations.

In 2020, the OIG started an information security inspection program. These inspections assess whether VA facilities are meeting federal security requirements related to three control areas in which the OIG determined risk is highest. Typically, facilities selected for these inspections either were not included in the annual audit sample or had previously performed poorly. Appendix B presents background information on federal information security requirements.

The OIG conducted this inspection to determine whether the Battle Creek Healthcare System in Michigan was meeting federal security guidance. The OIG selected the Battle Creek Healthcare System because it had not been recently visited as part of the annual FISMA audit. This inspection's scope and methodology are described in appendix C.

The inspection focused on three security control areas:

1. **Configuration management controls**, which identify and manage security features for all hardware and software components of an information system.[3]
2. **Security management controls**, which "establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of the procedures."[4]

[1] Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. §§ 3551–3558; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2023*, Report No. 23-01105-69, May 14, 2024.

[2] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2023*.

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

[4] GAO, *FISCAM*.

3. **Access controls**, which provide reasonable assurance that computer resources are restricted to authorized individuals. Access includes physical and environmental controls associated with physical security such as authorization, visitors, monitoring, delivery, and removal.[5]

Without these critical controls, VA's systems would be at risk of unauthorized access that could compromise their integrity. Further, a cyberattack could disrupt access to, destroy, or allow malicious control of personal information belonging to VA patients, dependents, beneficiaries, employees, contractors, or volunteers. Although the findings and recommendations in this report are specific to the Battle Creek Healthcare System, other VA facilities could benefit from reviewing this information and considering these recommendations.

What the Inspection Found

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

Configuration Management Controls Had Three Deficiencies

The healthcare system had deficiencies in three configuration management controls:

- **Vulnerability remediation.** Results of vulnerability scans list the vulnerabilities identified on VA's network. The OIG's analysis of the Office of Information and Technology's (OIT) vulnerability scan results and the healthcare system's plans of action and milestones showed OIT did not create plans of action and milestones for vulnerabilities that persisted past VA deadlines of 60 days for critical and high vulnerabilities.[6]
- **System baseline configurations.** The OIG team found the healthcare system's servers were running software that was not configured according to approved security baselines.
- **Unauthorized software.** The healthcare system did not address unauthorized software on its network.

[5] GAO, *FISCAM*.

[6] A "plan of action and milestones" identifies the tasks needing to be accomplished, details the resources required to accomplish the tasks, lists the milestones for meeting the tasks, and sets completion dates for the milestones. NIST Computer Security Resource Center, *Glossary*, August 19, 2024. In April 2024, VA increased the time to remediate critical vulnerabilities from 30 days to 60 days. VA's Information Security Knowledge Service, "Security Controls Explorer," April 9, 2024.

Security Management Controls Had One Deficiency

A facility's security management program "should establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures."[7] The OIG identified one security management control deficiency at the Battle Creek Healthcare System involving how local biomedical staff relied on incomplete security remediation reports to manage vulnerabilities on medical devices.

Consequently, in June 2024, the inspection team identified 25 vulnerabilities on seven biomedical devices that were not tracked in security remediation reports utilized by biomedical staff. According to the reporting process, OIT should provide biomedical staff with Continuous Readiness in Information Security Program remediation reports that list vulnerabilities for biomedical devices at the facility. Subsequently, staff should report to OIT the actions taken to remediate the identified vulnerabilities. This process would result in the security issue being removed from future remediation reports. In this case, however, the issues were removed from the security remediation reports even though no actions had been taken to resolve the vulnerabilities. As a result, local biomedical staff were not aware that corrective actions did not occur and that the vulnerabilities were not remediated. This may result in the unavailability of medical devices, which could negatively affect patients' health.

Access Controls Had Three Deficiencies

Access controls provide reasonable assurance that computer resources are restricted to authorized individuals.[8] At the Battle Creek facility, the inspection team reviewed access to environmental control elements over the computer room, communications closets, and a file room. The team found deficiencies in physical access, environmental controls, and network segmentation—which means partitioning off areas of the VA network that contain sensitive special-purpose systems and medical devices. If the deficiencies are not corrected, the facility risks unauthorized access, disruption, and destruction of critical information technology (IT) resources.

What the OIG Recommended

The OIG recommended the assistant secretary for information and technology and chief information officer improve vulnerability management processes, implement a more effective

[7] GAO, *FISCAM*.

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

baseline configuration process, and improve the remediations reporting process for the Continuous Readiness in Information Security Program.[9]

The OIG also recommended the Battle Creek Healthcare System's director, in conjunction with the assistant secretary for information and technology, restrict access to the server room and communications closets; ensure network segmentation controls are applied to all parts of the network hosting sensitive special-purpose systems and medical devices; and implement improved, consistent environmental controls for network communications closets.

VA Management Comments and OIG Response

The acting assistant secretary for the Office of Information and Technology and chief information officer concurred with recommendations 1 through 6 and requested recommendations 1, 3, 4, 5, and 6 be closed due to completed corrective actions. To support the closure request, the acting assistant secretary provided sufficient evidence showing actions were taken to address recommendations 3, 4, 5, and 6. Therefore, the OIG considers recommendations 3, 4, 5, and 6 closed. However, for recommendation 1, while actions were taken to provide agency oversight of the vulnerabilities on the network, there are still 17 critical vulnerabilities on 12 hosts and 26 high vulnerabilities on 1,984 hosts that have been on the network for over 12 months.[10] As a result, the OIG considers recommendation 1 open. For recommendation 2, the planned corrective actions are responsive to the intent of the recommendation. The OIG will monitor implementation of the planned actions and will close recommendations 1 and 2 when VA provides evidence demonstrating progress in addressing the identified issues. The full text of the acting assistant secretary's response is included in appendix D.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations.

[9] 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.

[10] The oldest critical vulnerability has been on the network for 24 months, and the oldest high vulnerability has been on the network for 25 months. Furthermore, these remaining vulnerabilities include one critical vulnerability and one high vulnerability that the Cybersecurity & Infrastructure Security Agency identified as "known exploited" vulnerabilities.

Contents

Abbreviations

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

Introduction

Information security controls protect VA systems and data from unauthorized access, use, modification, and destruction. To determine compliance with the Federal Information Security Modernization Act of 2014 (FISMA), the VA Office of Inspector General (OIG) contracts with an independent public accounting firm that conducts an annual audit of VA's information security program and practices.[11] 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). Appendix A details the fiscal year (FY) 2023 FISMA audit recommendations.

In 2020, the OIG started an information security inspection program. These inspections provide recommendations to VA on enhancing information security oversight at local and regional facilities.[12] Appendix B presents information about FISMA and other federal criteria and standards discussed in this report. Typically, facilities selected for these inspections either were not included in the annual FISMA sample or had previously performed poorly. Appendix C provides more detail on this inspection's scope and methodology.

The OIG conducted this inspection to determine whether the Battle Creek Healthcare System in Michigan was meeting federal security guidance. The OIG selected the Battle Creek Healthcare System because it had not been recently visited as part of the annual FISMA audit. Although the findings and recommendations in this report are specific to the Battle Creek Healthcare System, other facilities across VA could benefit from reviewing this information and considering these recommendations.

Security Controls

Both OMB and NIST provide criteria for implementing security controls.[13] These criteria call for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system.

[11] Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. §§ 3551–3558; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2023*, Report No. 23-01105-69, May 14, 2024.

[12] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2023.*

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

VA guidance outlines both NIST- and VA-specific requirements to help information system owners select the appropriate controls to secure their systems.[14] According to VA Directive 6500, responsibility for developing and maintaining information security policies, procedures, and control techniques lies with the assistant secretary for information and technology, who also serves as VA's chief information officer. VA Handbook 6500 describes the risk-based process for selecting system security controls, including operational requirements.

This OIG information security inspection focused on three security control areas selected based on their level of risk, as shown in table 1.

Table 1. Security Controls Evaluated by the OIG

Control area	Purpose	Examples evaluated
Configuration management	Identify and manage security features for all hardware and software components of an information system	Component inventory, baseline configurations, configuration settings, change management, vulnerability management, and flaw remediation
Security management	Establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of the procedures	Risk management, assessment, authorization, and monitoring
Access	Provide reasonable assurance that computer resources are restricted to authorized individuals	Access, identification, authentication, audit, and accountability—including related physical security controls

Source: VA OIG analysis.

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

[14] VA Handbook 6500, *Risk Management Framework for VA Information Systems: VA Information Security Program*, February 2021; VA Directive 6500, *VA Cybersecurity Program*, February 24, 2021. The NIST Computer Security Resource Center's Glossary defines a system owner as a "person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system." "Glossary" (web page), NIST Computer Security Resource Center, accessed September 30, 2024, https://csrc.nist.gov/glossary/term/system_owner.

Office of Information and Technology Structure and Responsibilities

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

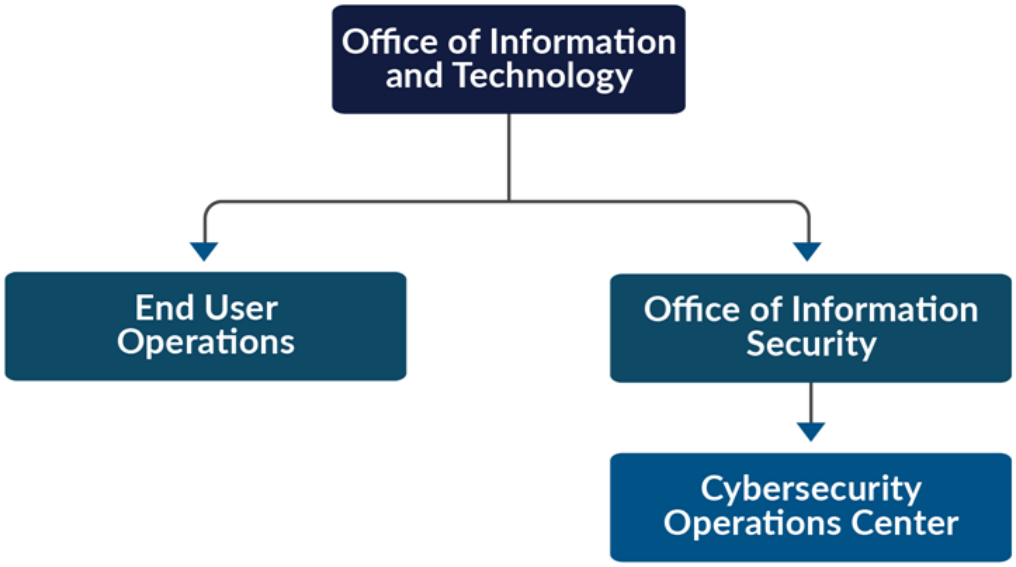

Figure 1. *Organizational structure of OIT entities relevant to this inspection.*
Source: VA OIG analysis.

OIT's End User Operations team provides on-site support to information technology (IT) customers across all VA administrations and program offices—including about 400,000 VA employees and about 100,000 contractors with government-furnished IT equipment and access. Further, End User Operations staff assigned to the Battle Creek Healthcare System are responsible for managing system plans of action and milestones to ensure all assessed and scanned vulnerabilities are documented.

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

Results of Previous Projects

The OIG's FY 2023 FISMA audit was conducted by independent public accounting firm CliftonLarsonAllen LLP. It evaluated 45 major applications and general support systems hosted

at 23 VA facilities and tested selected security and privacy controls outlined by NIST.[15] CliftonLarsonAllen LLP made 25 recommendations, which are listed in appendix A. All 25 recommendations were repeated from the prior annual audit—indicating VA continues to face significant challenges in complying with FISMA requirements.[16] Repeat recommendations included addressing deficiencies in configuration management, security management, and access controls.

The Government Accountability Office (GAO) has also found VA has a deficient information security program. GAO noted in 2019 that VA faced several security challenges while securing and modernizing its information systems, including

- effectively implementing information security controls,
- mitigating known vulnerabilities,
- establishing elements of its cybersecurity risk management program,
- identifying critical cybersecurity staffing needs, and
- managing IT supply chain risks.[17]

The Battle Creek Healthcare System

The Battle Creek Healthcare System consists of the Battle Creek VA Medical Center (shown in figure 2) and the Benton Harbor, Century Avenue, Lansing, Muskegon, and Wyoming VA clinics. According to an OIT representative, in FY 2023, the medical center provided care to 45,000 patients; housed 136 beds, including 75 community living beds; and had 2,021 employees. According to the same OIT representative, the medical center's budget for FY 2024 was $616 million.

[15] OMB, "Security of Federal Automated Information Resources," app. III in OMB Circular A-130, *Managing Information as a Strategic Resource*, November 28, 2000. The appendix in this OMB document defines a general support system as an interconnected set of information resources under the same direct management control that share common functionality.

[16] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2023*. See appendix A for a summary of recommendations made in that report and see appendix B for more information about FISMA and other requirements.

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

Figure 2. *Battle Creek VA Medical Center, Michigan.*
Source: Battle Creek Healthcare System Information System Security Officer, July 18, 2024.

Results and Recommendations

I. Configuration Management

According to the GAO's *Federal Information System Controls Audit Manual* (*FISCAM*), configuration management involves identifying and managing security features for all hardware, software, and firmware components of an information system at a given point and systematically controlling changes to that configuration during the system's operation.[18] An effective configuration management process should be described in a configuration management plan and then implemented according to that plan.

OIT's Cybersecurity Operations Center identifies and reports on threats and vulnerabilities within VA. Vulnerabilities that cannot be remediated by OIT at the enterprise level are referred to OIT staff assigned to specific facilities for action. This helps to secure devices from attack.

The OIG inspection team examined whether the Battle Creek Healthcare System identified and remediated vulnerabilities within established times and configured its servers according to standards.

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

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

- **Vulnerability remediation.** Analysis of the OIT's vulnerability scan results and its plans of action and milestones showed the facility did not create plans of action and milestones for vulnerabilities persisting past the 60-day limit set by VA.[19]
- **System baseline configurations.** The OIG team found the healthcare system's servers were running software that was not configured according to approved security baselines.
- **Unauthorized software.** The healthcare system did not address unauthorized software on its network.

[18] Firmware refers to computer programs and data stored in hardware, typically in read-only memory, that cannot be written or changed during the execution of the program. GAO, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G, February 2009.

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

Vulnerability Remediation

VA's vulnerability management program needs improvement. FISMA audits have repeatedly found deficiencies in the department's vulnerability management controls.[20] Consistent with those findings, the team identified deficient controls at the Battle Creek Healthcare System.

Vulnerability management is how an organization identifies, classifies, and reduces weaknesses. This management helps organizations assess risks and monitor the effectiveness of its overall security program. At VA, OIT conducts both routine and random vulnerability scans, and reports the identified vulnerabilities to facilities for remediation. In calendar year 2023, OIT implemented a formal process to track the monitoring and remediation of vulnerabilities by using a plan of action and milestones. However, as of this inspection, the new process had not been in place long enough to demonstrate effectiveness at remediating security vulnerabilities.

The new tracking process makes information stewards responsible for entering all critical and high-severity vulnerabilities that cannot be remediated on time (within 60 days) into a plan of action. The new process tracks vulnerability remediation efforts and extends the remediation time frames. Information stewards should then use a prescribed form to provide evidence showing that the deficiencies have been mitigated.[21]

NIST guidance calls for a severity level to be assigned to each vulnerability using the Common Vulnerability Scoring System.[22] The inspection team's testing of vulnerability remediation focused on whether critical and high vulnerabilities were remediated within agency-approved timelines, as shown in table 2.

[20] GAO, *FISCAM*. Vulnerabilities are "weaknesses in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source."

[21] According to the NIST Computer Security Resource Center Glossary, an information steward is "an agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal." "Glossary" (web page), NIST Computer Security Resource Center, accessed August 27, 2024, https://csrc.nist.gov/glossary/term/information_steward

[22] "Vulnerability Metrics" (web page), NIST National Vulnerability Database, accessed August 27, 2024, https://nvd.nist.gov/vuln-metrics/cvss; "Common Vulnerability Scoring System ver. 3.1, Specification Document, Revision 1," Forum of Incident Response and Security Teams, accessed August 27, 2024, https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf.

Table 2. Vulnerability Remediation Timelines by Severity Level

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

Source: VA OIG analysis of VA's Information Security Knowledge Service, "Security Controls Explorer," April 9, 2024.

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

The inspection team compared the results of the OIT-provided network vulnerability scan from the Battle Creek Healthcare System against OIG scans conducted from June 24, 2024, through June 27, 2024. OIT and the inspection team used the same vulnerability scanning tools; the OIG found no material differences between the two network scans. Both scans showed a high number of vulnerabilities persisting past deadlines.

As of June 2024, the Battle Creek Healthcare System had 64 critical vulnerabilities on 1,172 hosts and 192 high vulnerabilities on 3,850 hosts persisting past the VA-established deadlines. These vulnerabilities include 20 hosts using software that was no longer supported by the vendor and 15 vulnerabilities for which system stewards had not developed plans of action and milestones for remediation.

System Baseline Configuration

During the inspection, the team also scanned the configurable settings of the healthcare system's servers to check compliance with secure baselines. According to VA policy, these servers should be securely configured as part of the standard system development process, and systems should be configured using baselines that have been documented, formally reviewed, and agreed on by managers. But the OIG noted that certain software configuration settings did not meet baseline security requirements. Specifically, the OIG team identified

- 15 distinct, category 1 security configuration failures on 33 percent of hosts; and
- 18 distinct, category 2 security configuration failures on 40 percent of hosts.[23]

[23] Defense Information Systems Agency, *Application Security and Development Security Technical Implementation Guide Overview*, ver. 6, rev. 1, July 24, 2024.

Category 1 failures could allow primary security protections to be bypassed, inviting immediate access by unauthorized staff or an unauthorized assumption of superuser privileges. Category 2 failures have the potential for unauthorized system access or activity. Given the potential severity of such failures, security configuration of servers is not just a defensive strategy but also a proactive one that helps protect the confidentiality, availability, and integrity of VA systems.

Unauthorized Software

OIT uses endpoint management software to report unapproved software on computers. Reports for the Battle Creek network identified 3,873 unapproved versions of 95 software products that were installed on 2,647 of the healthcare system's computers. But the system's OIT employees did not review the reports for actions to be taken to address the unapproved software. The software was installed without proper authorization from OIT's project development team without a plan of action and milestones to mitigate any security deficiencies.[24] By not reviewing reports on unapproved software, VA has no assurance that corresponding system security and privacy plans have identified appropriate security controls for all components at the Battle Creek facility. Continuous monitoring bolsters ongoing awareness of system security and privacy issues and also supports risk management.[25]

Finding 1 Conclusion

Numerous system vulnerabilities were not mitigated on time, and software did not meet baseline requirements. These vulnerabilities created security weaknesses on the Battle Creek Healthcare System's network that could be exploited by malicious individuals to gain unauthorized access to sensitive information or disrupt operations. Further, OIT did not take actions to address unauthorized software installed on computers within the Battle Creek Healthcare System.

Recommendations 1–2

The OIG made the following recommendations to the assistant secretary for information and technology and chief information officer:[26]

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

[24] VA Technical Reference Model, ver. 24.10. VA allows unauthorized software if there is a signed plan of action and milestones to document the acceptance of risk.

[25] GAO, *FISCAM*.

[26] 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.

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

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

VA Management Comments

The acting assistant secretary for information and technology and chief information officer concurred with recommendations 1 and 2. For recommendation 1, the acting assistant secretary indicated there is a process in place to identify and age vulnerabilities and manage vulnerabilities that fall out of compliance with the VA-established time frames with a plan of action and milestones. Further, these corrective actions were completed on January 31, 2025. As a result, the acting assistant secretary requested that recommendation 1 be closed. In response to recommendation 2, the acting assistant secretary indicated OIT has implemented a process to identify, track, and remediate unauthorized software and ensure approval of baselines. The acting assistant secretary indicated that all identified unauthorized software will be remediated by the end of April 2025. The full text of the acting assistant secretary's response is included in appendix D.

OIG Response

For recommendation 1, while actions were taken to provide the agency oversight into the vulnerabilities on the network, there are still 17 critical vulnerabilities on 12 hosts and 26 high vulnerabilities on 1,984 hosts that have been on the network for over 12 months.[27] Therefore, the OIG considers recommendation 1 open. For recommendation 2, the planned corrective actions are responsive to the intent of the recommendation. The OIG will monitor implementation of the planned actions and will close recommendations 1 and 2 when VA provides evidence demonstrating progress in addressing the issues identified.

[27] The oldest critical vulnerability has been on the network for 24 months, and the oldest high vulnerability has been on the network for 25 months. Furthermore, these remaining vulnerabilities include one critical vulnerability and one high vulnerability that the Cybersecurity & Infrastructure Security Agency identified as "known exploited" vulnerabilities.

II. Security Management

According to *FISCAM*, security management controls establish a framework and a continuous cycle for assessing risk, developing security procedures, and monitoring the effectiveness of the procedures.[28] The inspection team evaluated network user management and vulnerability reporting at the Battle Creek Healthcare System.

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

To assess security management controls, the inspection team reviewed local security management policies, standard operating procedures, and applicable VA policies. These included documentation from the Enterprise Mission Assurance Support Service, VA's cybersecurity management service for workflow automation and continuous monitoring. The team interviewed the information systems security manager, information system security officers, biomedical staff, and the area manager. The team also conducted a walk-through of the Battle Creek facility. Security management controls reviewed included user management and oversight of medical devices.

Improvements Are Needed in Reporting Vulnerabilities for Medical Devices

The OIG identified one security management control deficiency at the Battle Creek Healthcare System involving how local biomedical staff relied on incomplete security remediation reports to manage vulnerabilities on medical devices. Consequently, in June 2024, the inspection team identified 25 vulnerabilities on seven biomedical devices that were not tracked in security remediation reports utilized by local biomedical staff. According to the reporting process, OIT should provide biomedical staff with Continuous Readiness in Information Security Program remediation reports that list vulnerabilities for biomedical devices at the facility. Staff are then expected to report to OIT the actions taken to remediate the identified vulnerabilities. This process should result in the security issue being removed from future remediation reports. In this case, however, the issues were removed from the security remediation reports even though no actions had been taken to resolve the vulnerabilities. As a result, local biomedical staff were not aware that corrective actions did not occur and that the vulnerabilities were not remediated. This may result in the unavailability of medical devices, which could negatively affect patients' health.

[28] GAO, *FISCAM*.

Finding 2 Conclusion

Improvements are needed to address how OIT reports vulnerabilities on medical devices at the Battle Creek Healthcare System. Without effective vulnerability reporting, managers may be unaware that remediation efforts either were not implemented or were not successful at remediating vulnerabilities. This may result in the unavailability of medical devices, which could negatively affect patients' health.

Recommendation 3

The OIG made the following recommendation to the assistant secretary for information and technology and chief information officer:[29]

3. Improve the remediations reporting process for the Continuous Readiness in Information Security Program to verify that corrective actions are taken to fully mitigate vulnerabilities for biomedical devices at the Battle Creek facility.

VA Management Comments

The acting assistant secretary for information and technology and chief information officer concurred with recommendation 3. The acting assistant secretary indicated OIT has implemented a reporting process to verify that corrective actions are taken to mitigate vulnerabilities for the facility's medical devices. Furthermore, the vulnerabilities identified in the report were remediated, with corrective actions completed on February 10, 2025. The full text of the acting assistant secretary's response is included in appendix D.

OIG Response

For recommendation 3, the planned corrective actions are responsive to the intent of the recommendation. The acting assistant secretary provided sufficient evidence to support that actions taken in response to recommendation 3 were complete. The OIG considers recommendation 3 closed.

[29] 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

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

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

Identification, authentication, and authorization controls ensure users have proper access and that access is restricted to authorized individuals. At the Battle Creek Healthcare System, the inspection team reviewed access and environmental controls over the computer room and communications closets.[30]

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

To evaluate the Battle Creek Healthcare System's access controls, the inspection team interviewed OIT and facility staff, reviewed local policies and procedures, and conducted walk-throughs of the facility.[31] The OIG found problems with physical access controls, network segmentation controls, and environmental controls.

Physical Access Controls

The inspection team discovered that physical access to the Battle Creek facility and its IT resources was not effectively controlled. Physical access controls include devices and barriers to prevent movement from publicly accessible areas to nonpublic areas.[32] At the time of this inspection, the facility had an automated physical access control system that allowed individuals with badges to enter the server room and communications closets and also allowed employees with keys to access the server room and communications closets.

The OIG found that badge access to the server room was not adequately restricted. For example, the system allowed unnecessary access to the server room and communications closets to 119 individuals. These 119 individuals included six former employees. Furthermore, 20 VA fire staff and 22 VA police officers had access. After the inspection team reported these individuals'

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

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

[32] NIST Special Publication 800-53.

unauthorized access to the server room and communications closets, the facility removed or disabled access for 59 individuals—including the six former employees and three of the VA fire staff—and properly authorized 32 others. The inspection team met with facility personnel, who indicated they were still in the process of developing a method for controlling access for individuals who need only occasional access.

The OIG also found that, although the facility had a process for assigning keys to the communications closets, it did not keep an inventory to ensure all keys were on hand or issued only to authorized individuals. Keys were issued to 14 individuals who were not included on the access authorization memo. Facility staff said the facility was ending key access and transitioning to an automated physical access control system that restricts badge access to the server room and communications closets.

Network Segmentation Controls

At VA, network segmentation means partitioning off areas of the network that contain sensitive special-purpose systems and medical devices. The OIG team found the Battle Creek Healthcare System did not have network segmentation controls in place for several medical and special-purpose system segments.[33]

Network segmentation controls regulate where information can travel within a system and between systems.[34] Network-connected medical devices and special-purpose systems are placed on isolated network segments for protection. This protection is provided through access control lists, which limit the resources that can be accessed within each network segment. However, the OIG identified three network segments containing 54 special-purpose systems and medical devices that did not have access control lists applied to restrict access.

Without adequate network segmentation, any VA network user can access vulnerable medical devices or special-purpose systems, increasing the risk of a device being compromised by a malicious user. This could negatively affect patients' health and safety.

Environmental Controls

The team tested 10 of the 50 communications closets at the Battle Creek facility and found that they did not meet federal and VA environmental security requirements related to an uninterruptible power supply and grounding of equipment.

[33] The medical device segment was at the Muskegon VA Clinic, which opened a month prior to the site inspection on a device that OIT representatives had indicated was misconfigured.

[34] NIST Special Publication 800-53.

Uninterruptible power supplies provide emergency power when the main power source fails.[35] They are used to protect devices and telecommunications equipment from unexpected disruption, which could cause injuries or death, disrupt business operations, or result in losses in data or information. Uninterruptible power supplies differ from emergency power systems for backup generators because they provide near-instantaneous protection from interruptions. But without operational uninterruptible power supplies, VA equipment will not function during power fluctuations or outages, resulting in interrupted data flow and disrupted access to network resources. This could pose a risk to patient health.

VA also requires telecommunications equipment to be properly grounded because without proper grounding, the equipment could be damaged by electromagnetic interference and power surges. The OIG team found the following:

- Power in three of the 10 communications closets inspected was not safeguarded with functioning devices to guarantee an uninterruptible power supply during a prolonged outage. Specifically, two had uninterruptible power supply devices that needed to be serviced, and one had an uninterruptible power supply device that was not installed.
- Equipment was not grounded in six of the 10 communications closets the team inspected. The staff at the Battle Creek facility were unaware that equipment was not grounded.[36]

Not having adequate uninterruptible power supply coverage or a properly grounding network could have a negative impact on the facility's ability to provide health care, thereby negatively affecting patient health.

Finding 3 Conclusion

The Battle Creek Healthcare System's access controls did not restrict physical or logical access to computer resources, leaving them unprotected from theft and intentional or accidental damage. Additionally, environmental controls were not consistently implemented to safeguard equipment in communications closets. If the deficiencies are not corrected, the facility risks unauthorized access, disruption, and destruction of critical IT resources.

[35] NIST Special Publication 800-53.

[36] NIST Special Publication 800-53; VA, Telecommunications and Special Telecommunications Systems Design Manual, February 2016, https://www.cfm.va.gov/til/dManual/dmTelecomm.pdf.

Recommendations 4–6

The OIG made three recommendations to the VA Battle Creek Healthcare System's director, in conjunction with the assistant secretary for information and technology and chief information officer:[37]

4. Implement improved physical access controls to restrict access to the server room and communications closets.
5. Ensure network segmentation controls are applied to all network segments hosting special-purpose systems or medical devices.
6. Implement improved, consistent environmental controls for network communications closets.

VA Management Comments

The acting assistant secretary for the Office of Information and Technology and chief information officer concurred with recommendations 4, 5, and 6 and requested these recommendations be closed due to completed corrective actions. For recommendation 4, the acting assistant secretary reported OIT reviewed and updated access control lists to the server rooms and all communications closets on December 17, 2024, restricting access to only authorized individuals, and will conduct reviews on a biannual basis. Regarding recommendation 5, the acting assistant secretary stated OIT implemented the necessary segmentation controls for the network segments that host special-purpose systems and medical devices on February 7, 2025. For recommendation 6, the acting assistant secretary indicated the facility completed a review of network communications closets to consistently implement the required environmental controls on January 31, 2025. The full text of the acting assistant secretary's response is included in appendix D.

OIG Response

For recommendations 4, 5, and 6, the planned corrective actions are responsive to the intent of the recommendations. The acting assistant secretary provided sufficient evidence to support those actions taken in response to recommendations 4, 5, and 6 were complete. Therefore, the OIG considers recommendations 4, 5, and 6 closed.

[37] 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.

Appendix A: Recommendations from FISMA Audit for FY 2023 Report

In the Federal Information Security Act of 2014 (FISMA) audit for fiscal year (FY) 2023, CliftonLarsonAllen LLP made 25 recommendations.[38] All 25 were repeat recommendations from the prior year. The FISMA audit assesses the VA-wide security management program, and recommendations in the FISMA report are not specific to the Battle Creek Healthcare System. Recommendations 9 and 10 were made to the Office of Personnel Security, Human Resources, and Contract Offices.[39] The remaining 23 recommendations were made to the assistant secretary for information and technology. All recommendations are listed below.

1. Improve continuous monitoring program in accordance with the NIST Risk Management Framework. Specifically, implement an independent security control assessment process to evaluate the effectiveness of security controls prior to granting authorization decisions.
2. Implement improved mechanisms to ensure system stewards and Information System Security Officers follow procedures for establishing, tracking, and updating Plans of Action and Milestones for all known risks and weaknesses including those identified during security control assessments.
3. Implement controls to ensure that system stewards and responsible officials obtain appropriate documentation prior to closing Plans of Action and Milestones.
4. Develop mechanisms to ensure system security plans reflect current operational environments, include an accurate status of the implementation of system security controls, and all applicable security controls are properly evaluated.
5. Implement improved processes for reviewing and updating key security documentation, including control assessments on a risk-based rotation or as needed. Such updates will ensure all required information is included and accurately reflects the current environment.
6. Implement improved processes to ensure compliance with VA password policy and security standards on domain controls, operating systems, databases, applications, and network devices.

[38] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2023*, Report No. 23-01105-69, May 14, 2024.

[39] Recommendations 9 and 10 were addressed by the assistant secretary for information and technology.

7. Implement periodic reviews to minimize accounts and permissions in excess of required functional responsibilities and remove unauthorized or unnecessary accounts.
8. Enable system audit logs on all critical systems and platforms and conduct centralized reviews of security violations across the enterprise.
9. Implement improved processes for establishing and maintaining accurate investigation data within VA systems used for background investigations.
10. Strengthen processes to ensure appropriate levels of background investigations are completed for applicable VA employees and contractors.
11. Implement more effective automated mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and web application servers.
12. Implement improved processes for tracking and resolving vulnerabilities that cannot be addressed within policy time frames. Implement more effective patch and vulnerability management processes to mitigate identified security deficiencies and reduce applicable security risks.
13. Maintain a complete and accurate security baseline configuration for all platforms and ensure all baselines are appropriately monitored for compliance with established VA security standards.
14. Implement improved controls that restrict vulnerable medical devices from unnecessary access to the general network.
15. Enhance procedures for tracking security responsibilities for networks, devices, and components not managed by the Office of Information and Technology to ensure vulnerabilities are remediated in a timely manner.
16. Implement improved processes to ensure that all devices and platforms are evaluated using credentialed vulnerability assessments.
17. Implement improved procedures to enforce standardized system development and change control processes that integrate information security throughout the life of each system.
18. Implement improved procedures to ensure that system outages and disruptions are tracked to specific system boundaries and that interdependent systems are considered for the purposes of tracking and measuring against stated system recovery time objectives.
19. Ensure contingency plans for all systems and applications are updated and tested in accordance with VA requirements.

20. Ensure that systems and applications are adequately logged and monitored to facilitate an agencywide awareness of information security events.
21. Implement improved safeguards to identify and prevent unauthorized vulnerability scans on VA networks.
22. Implement improved measures to ensure that all security controls are assessed in accordance with VA policy and that identified issues or weaknesses are adequately documented and tracked within Plans of Actions and Milestones.
23. Implement improved processes to monitor for unauthorized changes to system components and the installation of prohibited software on all agency devices and platforms.
24. Develop a comprehensive inventory process to identify connected hardware, software, and firmware used to support VA applications and operations.
25. Implement improved procedures for monitoring contractor-managed systems and services and ensure information security controls adequately protect VA sensitive systems and data.

Appendix B: Background

Federal Information System Controls Audit Manual (*FISCAM*)

The Government Accountability Office (GAO) developed *FISCAM* to give auditors and information system control specialists a specific methodology for evaluating the confidentiality, integrity, and availability of information systems. *FISCAM* groups controls based on similar risks.[40] To help auditors evaluate information systems, *FISCAM* aligns control categories with National Institute of Standards and Technology (NIST) controls.

FISCAM breaks configuration management controls into the following critical elements:

- **Develop and document configuration management policies, plans, and procedures** at the entity, system, and application levels to ensure effective configuration management processes. These procedures should cover employee roles and responsibilities, change control, system documentation requirements, establishment of decision-making structure, and configuration management training.
- **Maintain current configuration information,** which involves naming and describing physical and functional characteristics of a controlled item, as well as performing activities to define, track, store, manage, and retrieve configuration items. Examples of these controls are baseline configurations, configuration settings, and component inventories.
- **Authorize, test, approve, and track changes** by formally establishing a change management process, with manager authorization and approval of the changes. This element includes documenting and approving test plans, comprehensive and appropriate testing of changes, and creating an audit trail to clearly document and track changes.
- **Conduct routine configuration monitoring** to determine the accuracy of the changes that should address baseline and operational configuration of hardware, software, and firmware.[41] Products should comply with applicable standards and the vendors' good security practices. The organization should have the ability to monitor and test to determine whether a system is functioning as intended and to determine whether networks are appropriately configured, and paths are protected between information systems.

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

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

- **Update software on a timely basis** by scanning software and updating it frequently to guard against known vulnerabilities. In addition, security software should be kept current by establishing effective programs for patch management, virus protection, and identification of other emerging threats. Software releases should be controlled to prevent the use of noncurrent software. Examples of these controls are software usage restrictions, user-installed software, malicious code protection, security alerts, and advisories. Examples of controls in this element are vulnerability scanning, flaw remediation, malicious code protection, security alerts, and advisories.
- **Document and have emergency changes approved** by appropriate entity officials and notify appropriate staff for follow-up and analysis of the changes. It is not uncommon for program changes to be needed on an emergency basis to keep a system operating. However, because of the increased risk of errors, emergency changes should be kept to a minimum.[42]

FISCAM identifies the following critical elements for contingency planning:

- **A computerized operations criticality and sensitivity assessment** is a management analysis of data and operations to determine which are the most critical and what resources are needed to recover and support them.
- **Prevent and minimize damage and interruption** by implementing backup procedures and installing environmental controls. These controls are generally inexpensive ways to prevent relatively minor problems from becoming costly disasters. This control also includes effective maintenance, problem management, and change management for hardware.
- **A comprehensive contingency plan** or suite of related plans should be developed for restoring critical applications; this includes arrangements for alternate processing facilities in case the usual facilities are damaged or cannot be accessed.
- **Contingency testing** determines whether plans will function as intended and can reveal important weaknesses, which leads to plan improvement.[43]

FISCAM has seven critical elements for security management:

- **Institute a security management program** that establishes policies, plans, and procedures clearly describing all major systems and facilities and that outlines the duties of those responsible for overseeing security as well as those who own, use, or rely on the organization's computer resources. There should be a clear security

[42] GAO, *FISCAM*.
[43] GAO, *FISCAM*.

management structure for systems and devices as well as for business processes. Examples of specific controls are system security plans, plan updates, activity planning, and resource allocation.

- **Assess and validate risk** by comprehensively identifying and considering all threats and vulnerabilities. This step ensures agencies address the greatest risks and appropriately decide to accept or mitigate risks. Examples of these controls are security certification, accreditation, categorization, and risk assessment.
- **Document and implement security control policies and procedures** that appropriately address general and application controls and ensure users can be held accountable for their actions. These controls, which are more general at the entity-wide level and more specific at the system level, should be approved by managers.
- **Implement security awareness and personnel policies** that provide training for new employees, contractors, and users; periodic refresher training; and distribution of security policies detailing rules and expected behaviors. This element also addresses hiring, transfers, terminations, and performance for employees, contractors, and users. Examples of controls in this area are security awareness training, rules of behavior, position categorization, personnel policies, personnel screening, termination, transfer, access agreements, third-party personnel security, and personnel sanctions.
- **Monitor the program** to ensure policies and controls effectively reduce risk on an ongoing basis. Effective monitoring involves testing controls to evaluate and determine whether they are appropriately designed and operating effectively. Examples of these controls are security assessments, continuous monitoring, privacy impact assessments, and vulnerability scanning.
- **Remediate information security weaknesses** when they are identified, which involves reassessment of related risks, applying appropriate corrective actions, and follow-up monitoring to ensure actions are effective. Agencies develop plans of actions and milestones to track weaknesses and corresponding corrective actions.
- **Ensure third parties are secure,** as vendors, business partners, and contractors are often granted access to systems for purposes such as outsourced software development or system transactions.[44]

[44] GAO, *FISCAM*.

FISCAM lists six access control critical elements:

- **Boundary protection controls** protect a logical or physical boundary around a set of information resources and implement measures to prevent unauthorized information exchange across the boundary. Firewall devices are the most common boundary protection technology.
- **Sensitive system resources controls** are designed to ensure the confidentiality, integrity, and availability of system data such as passwords and keys during transmission and storage. Technologies used to control sensitive data include encryption and certificate management.
- **Physical security** restricts access to computer resources and protects them from loss or impairment. Physical security controls include guards, gates, locks, and environmental controls such as smoke detectors, fire alarms and extinguishers, and uninterruptible power supplies.
- **Audit and monitoring controls** involve the collection, review, and analysis of events for indications of inappropriate or unusual activity. These controls should be routinely used to assess the effectiveness of other security controls, to recognize an attack, and to investigate during or after an attack.
- **Identification and authentication controls** distinguish one user from another and establish the validity of a user's claimed identity.
- **Authorization controls** determine what users can do, such as granting access to various resources, and depend on valid identification and authentication controls. These controls establish the validity of a user's claimed identity.[45]

Federal Information Security Modernization Act (FISMA) of 2014

The following are the stated goals of FISMA:

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

[45] GAO, *FISCAM*.

- 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.[46]

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.

National Institute of Standards and Technology Information Security Guidelines

The National Institute of Standards and Technology (NIST) is responsible for developing tests, methods, and technical analyses for securing federal information systems. The Special Publication 800 series reports on NIST's research, guidelines, and outreach efforts in information systems security and privacy. The Federal Information Processing Standards Publication Series is the official series of publications related to standards and guidelines adopted under the Information Technology Management Reform Act of 1996 and the Federal Information Security Management Act (FISMA) of 2002.

[46] Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551.

Appendix C: Scope and Methodology

Scope

The VA Office of Inspector General (OIG) inspection team conducted its work from May 2024 through December 2024. The team evaluated configuration management, contingency planning, security management, and access controls of operational VA information security assets and resources in accordance with the Federal Information Security Modernization Act (FISMA), National Institute of Standards and Technology (NIST) security guidelines, and VA's information security policy. In addition, the team assessed the capabilities and effectiveness of information security controls used to protect VA systems and data from unauthorized access, use, modification, or destruction.

Methodology

To accomplish the objective, the inspection team examined relevant laws and policies and inspected the Battle Creek Healthcare System and its information systems for security compliance. Additionally, the team interviewed VA staff responsible for the facility's information technology security and operations. The team conducted vulnerability and configuration testing to determine local systems' security compliance. Finally, the team analyzed the results of testing, interviews, and the inspection to identify policy violations and threats to security.

Internal Controls

The inspection team determined internal controls were significant to the inspection's objectives. The overall scope of information security inspections is the evaluation of general security and application controls that support VA's programs and operations. According to the risk management framework for VA information systems, the information security program is the foundation for VA's information security and privacy program and practices. The framework is documented in VA Handbook 6500.

The team used the Government Accountability Office's *Federal Information System Controls Audit Manual (FISCAM)* as a template to plan the inspection. When planning for this inspection, the team identified potential information system controls that would significantly affect the review. Specifically, the team used the *FISCAM* appendix II as a guide to help develop evidence requests and interview questions for Battle Creek Healthcare System staff. The team used the *FISCAM* controls identified in appendix B of this report to determine the FISMA controls VA uses to protect and secure its information systems. Although similar to the contractor-conducted annual FISMA audits, this inspection focused on security controls that are implemented at the local level. However, some controls overlap and are included in both assessments due to

redundant roles and responsibilities among VA's local, regional, and national facilities and offices.

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

Data Reliability

The inspection team generated computer-processed data by using network scanning tools. The results of the scans were provided to OIT. The team used an industry-standard information system security tool to identify information systems on the VA network and to capture relevant configuration information, which is used to identify vulnerabilities and compliance with secure baselines. In this process, the team was not testing VA data or systems for transactional accuracy. The security tools identified a version of software present on a system and then compared it to the expected version. If the system did not have the current software version, the tool identified that as a vulnerability. The team relied on the results of the scanning tool and network device configuration. The team performed its own scans to determine whether the agency scans were complete and accurate, met intended purposes, and were not subject to alteration. The team did not find any material differences between OIG and agency scan data and determined the data used were complete and accurate.

Government Standards

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

Appendix D: VA Management Comments

Department of Veterans Affairs Memorandum

Date: March 13, 2025

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

Subj: Inspection of Information Security at the Battle Creek Healthcare System in Michigan (Draft Report) (VIEWS 12552570)

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

1. Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft report, Inspection of Information Security at the Battle Creek Healthcare System in Michigan (Project Number OIG-2024-02575-AE-0098).

2. The Office of Information and Technology (OIT) submits the attached written comments. OIT acknowledges the OIG's findings, concurs with the OIG's recommendations, and provides a corrective action plan and target implementation date or closure evidence for each OIG recommendation to the Department.

The OIG removed point of contact information prior to publication.

(Original signed by)

Eddie Pool

Attachment

Attachment

Office of Information and Technology

Comments on Office of Inspector General Draft Report,

"Inspection of Information Security at the Battle Creek Healthcare System in Michigan"

Project Number 2024-02575-AE-0098

(VIEWS 12552570)

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

Comments: The Department of Veterans Affairs (VA) Office of Information and Technology (OIT) concurs. OIT has processes in place to identify and maintain aged vulnerabilities in the critical, high, and medium categories. OIT will document and manage vulnerabilities that fall out of compliance with the VA established time frames with a Plan of Action and Milestone.

Expected Completion Date: Completed. Completion date: January 31, 2025.

VA requests closure recommendation 1.

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

Comments: Concur. OIT has implemented a process to identify, track, and remediate unauthorized software and ensure approval of baselines. All identified unauthorized software is scheduled for removal.

Expected Completion Date: April 30, 2025.

Recommendation 3: Improve the remediations reporting process for the Continuous Readiness in Information Security Program to verify that corrective actions are taken to fully mitigate vulnerabilities for biomedical devices at the Battle Creek facility.

Comments: Concur. OIT has implemented a reporting process to verify that corrective actions are taken to fully mitigate vulnerabilities for biomedical devices at the facility. OIT remediated all identified vulnerabilities.

Expected Completion Date: Completed. Completion date: February 10, 2025.

VA requests closure of recommendation 3.

Recommendation 4: Implement improved physical access controls to restrict access to the server room and communications closets.

Comments: Concur. OIT reviewed and updated access control lists to restrict access to the server rooms and all communications closets, thereby ensuring that only individuals with approved authorization can access secured areas.

Expected Completion Date: Completed. Completion date: December 17, 2024.

VA requests closure of recommendation 4.

Recommendation 5: Ensure network segmentation controls are applied to all network segments hosting special-purpose systems or medical devices.

Comments: Concur. OIT implemented a process to apply the necessary network segmentation controls for the network segments that host special-purpose systems and medical devices. OIT completed segmentation for all identified devices.

Expected Completion Date: Completed. Completion date: February 7, 2025.

VA requests closure of recommendation 5.

Recommendation 6: Implement improved, consistent environmental controls for network communications closets.

Comments: Concur. The facility conducted a review of network communications closets to consistently implement required environmental controls. Controls are implemented for all equipment.

Expected Completion Date: Completed. Completion date: January 31, 2025.

VA requests closure of recommendation 6.

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

OIG Contact and Staff Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Inspection Team	Michael Bowman, Director Sachin Bagai Nicholas Hartzheim Albert Schmidt Justin Skeen Brandon Zahn
Other Contributors	Rashiya Washington

Report Distribution

VA Distribution

Office of the Secretary
Veterans Benefits Administration
Veterans Health Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel
Office of Acquisition, Logistics, and Construction
Board of Veterans' Appeals
Director, Battle Creek Healthcare System

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Government Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget
US Senate: Gary Peters, Elissa Slotkin
US House of Representatives: Tom Barrett, Bill Huizenga, John Moolenaar, Hillary Scholten, Tim Walberg