US DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS HEALTH ADMINISTRATION

Inspection of Information Security at the VA Bedford Healthcare System in Massachusetts

Information Security Inspection	**23-02330-127**	**June 5, 2024**

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 technology (IT) controls protect VA systems and data from unauthorized access, use, modification, or 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.[1] The FISMA audit is conducted in accordance with guidelines issued by the Office of Management and Budget and applicable National Institute of Standards and Technology (NIST) information security guidelines.[2]

The fiscal year (FY) 2022 FISMA audit indicated that VA continues to face significant challenges meeting the law's requirements. The audit made 26 recommendations to VA. Repeat recommendations included addressing deficiencies in configuration management, contingency planning, security management, and access controls.[3] Appendix A details these recommendations.

In 2020, the OIG also started an information security inspection program. These inspections assess whether VA facilities are meeting federal security requirements related to three control areas the OIG determined to be at highest risk.[4] 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 Bedford VA Healthcare System in Massachusetts was meeting federal security guidance. The OIG selected the Bedford VA Healthcare System because it had not been recently visited as part of the annual FISMA audit. The inspection scope and methodology are described in appendix C.

The OIG's inspections are focused on the following three security control areas:

1. **Configuration management controls** identify and manage security features for all hardware and software components of an information system.[5]

[1] Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551–3558.

[2] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2022*, Report No. 22-01576-72, May 17, 2023.

[3] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2022.*

[4] The OIG recently removed a fourth control area—contingency planning—from its information security inspections because this area is largely enterprise controlled and not a significant risk at the local level. Appendix B presents background information on federal information security requirements.

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

2. **Security management controls** "establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of the procedures."[6]
3. **Access controls** provide reasonable assurance that computer resources are restricted to authorized individuals. Access also includes physical and environmental controls associated with physical security, such as authorization, visitors, monitoring, delivery, and removal.[7]

Although the findings and recommendations in this report are specific to the Bedford VA Healthcare System, other facilities across VA 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 Two Deficiencies

The Bedford VA Healthcare System had deficiencies in two configuration management controls:

- Configuration monitoring is the process by which the organization monitors the baseline and operational configuration of hardware, software, and firmware.
- System Life-Cycle Management is how organizations update software on a timely basis to guard against known vulnerabilities.[8]

Database Configuration Monitoring

Prior FISMA audits have repeatedly found deficiencies in VA's configuration management process by which the Office of Information and Technology (OIT) identifies, classifies, and reduces weaknesses. The inspection team identified 10 instances where databases were hosting personally identifiable information that was not monitored with OIT's quarterly compliance scans to detect unresolved security issues. While the database servers were reimaged within the last six months, without quarterly compliance scans management has no assurance that these databases are configured in compliance with VA configuration security baselines. The inspection team evaluated the servers and found approximately 66 percent of the databases did not meet VA's configuration baselines because they were not scanned for vulnerabilities and were not

[6] GAO, *FISCAM*.

[7] GAO, *FISCAM*.

[8] NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations,* September 23, 2021.

configured to capture audit logs. OIT representatives said it is the responsibility of healthcare system personnel to request compliance scans for databases owned and maintained by the facility or their contractors. Further, the facility could not provide evidence that audit logs for these databases were captured. As a result, user account access to these databases was not monitored for unauthorized access. Without effective database monitoring, there is an increased risk that a data breach of personally identifiable information could occur and go undetected.

System Life-Cycle Management

The inspection team noted that about 87 percent of the healthcare system's network devices used operating systems that did not meet baseline security requirements. Further, 4 percent of these network devices were at the end of their useful life and no longer received maintenance support from the vendor. Moreover, there were 12 vulnerabilities spread over the 4 percent of network devices that contained vulnerabilities identified by the Cybersecurity and Infrastructure Security Agency as known exploited vulnerabilities that needed to be remediated by all federal civilian executive branch agencies.[9] The facility's IT staff pointed out that the outdated software was allowed based on VA procedure; however, VA policy states, "Do not use unsupported EOL [end of life] software," as a best practice.[10] Deficient devices that did not meet VA baseline security configurations should have been updated with vendor-supported systems software during the standard system development life-cycle process. Upgrading is a proactive strategy to protect network stability and ensure security and privacy.

Security Management Controls Had Three Deficiencies

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."[11] The OIG identified three security management control deficiencies at the VA Bedford Healthcare System: authorization to operate, security categorization, and continuous monitoring of the Lynx Duress panic button system to verify that it contains complete and accurate user location information.

The OIG determined that the VA Bedford Healthcare System's special-purpose systems did not have an authorization to operate because they had not cleared the NIST risk management

[9] This remediation mandate is in accordance with Department of Homeland Security, Binding Operational Directive 22-01, *Reducing Significant Risk of Known Exploited Vulnerabilities*, November 3, 2021.

[10] Local Area Network (LAN) Security Configuration Baseline, version 1.0, dated September 28, 2021. Vulnerability Management End of Life Policy, June 13, 2023.

[11] GAO, *FISCAM*.

framework.[12] OIT issues an authorization to operate an information system and explicitly accepts the risk to agency operations, assets, individuals, or other organizations based on the implementation of approved security and privacy controls.[13] Without an authorization to operate, facility managers do not have assurance that the implemented security and privacy controls reduce the risk of a system compromise to an acceptable level. A compromise of the special-purpose systems' security could threaten the safety of patients, staff members, and visitors.

The VA Bedford Healthcare System was one of the 137 VA healthcare systems that owned special-purpose systems for which OIT did not consider all information types when establishing a consolidated security category level. The OIG previously identified this issue during its information security inspection of the VA Beckley Healthcare System in West Virginia.[14] NIST's risk management framework requires the baseline controls for information systems be set based on the system's security categorization. The security categorization is determined by the risk of loss of confidentiality, integrity, and availability of the information within each system. The system's security categorization—low, medium, or high—is used to select the system's security controls.

OIT used a single standard for all special-purpose systems, and the security categorization only included the "general information" type. As a result, managers assigned those special-purpose systems a security risk categorization of low for confidentiality, moderate for integrity, and moderate for availability. However, the inspection team determined that the special-purpose systems at Bedford included a system that warranted higher security levels: a network panic button system, which falls under the "emergency-response information" type, should have a security categorization of low for confidentiality, high for integrity, and high for availability, as recommended by NIST.[15]

Although NIST allows the security categorization to be adjusted, OIT would need to document the rationale or justification for adjustments, which was not done. Furthermore, the VA Bedford Healthcare System's special-purpose systems' security plan only considered security controls based on the lower security categorization developed by OIT. By not considering all information

[12] VA's Enterprise Mission Assurance Support Service indicates the special-purpose system "is comprised of operational technology devices/systems that assist, support, and maintain mission capabilities and operations for building safety, healthcare services, security services and other general services functional support areas." The NIST risk management framework provides a process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle. Managing organizational risk is paramount to effective information security and privacy programs.

[13] Office of Management and Budget Circular A-130, app. 2, July 28, 2016.

[14] VA OIG, *Inspection of Information Security at the VA Beckley Healthcare System in West Virginia*, Report No. 23-00089-144, September 20, 2023.

[15] NIST Special Publication 800-60, Vol 1, Rev 1, *Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices*, August 2008.

types during the security categorization, healthcare system leaders do not have assurance that appropriate security and privacy controls for special-purpose systems reduce the risk of compromise to an acceptable level.

Lynx Duress is a panic button system for users to send a silent alarm alerting VA facility police if there is an emergency situation that requires their immediate attention. The inspection team determined that improvements are needed for monitoring user locations within the Lynx Duress system. VA's domain infrastructure division chief said local OIT personnel once maintained the user location information for the panic button system; however, the responsibility was shifted to users. VA police stated that users ignore prompts to enter location information. Within the past year, only about 60 to 74 percent of users had completed monthly automated tests of the systems to ensure accurate location information. The lack of updated user locations could cause delays in police response and potentially allow life-threatening injuries.

Access Controls Had Four Deficiencies

Access controls provide reasonable assurance that computer resources are restricted to authorized individuals. At the Edith Nourse Rogers Memorial Veterans' Hospital, the main facility in the VA Bedford Healthcare System, the inspection team reviewed two critical access control elements: access controls and environmental controls. The inspection team found deficiencies in four access control areas: restricting physical access, monitoring of physical access, and implementing appropriate physical controls and environmental controls.[16]

Physical Building Access

The inspection team found that physical access to the facility and IT resources was not effectively controlled. The automated system required badges to enter the server room. The team found 39 individuals who should not have had access to the server room were granted the ability to enter the room with their badges. These 39 individuals included 10 former employees.[17] Further, communication closets had proximity card devices that were not functioning to restrict and record physical access. No corresponding plan of action and milestones was initially created to address the faulty badge reader devices until after the OIG announced its plan to conduct an information security inspection. To compensate for the deficiency, the facility relied on key access to communication closets, but process controls over key inventory were inadequate. For example, the inventory of master keys had not been taken since 2009. Since this issue was identified, the master key inventory was reduced from 41 to 27 keys.

[16] Environmental controls include electrical grounding, fire protection, and temperature and humidity controls.

[17] Healthcare system IT personnel indicated that they collect badges from employees when their employment is terminated, and the individuals with access did not utilize the access.

Monitoring of Server Room and Communication Closets

The OIG determined that the hospital video surveillance system did not monitor the server room and communication closet. The electronic badging access system allows monitoring of the server room access, which also requires video surveillance; however, it does not monitor access to the communication closets.

Emergency Power Controls

An uninterruptible power supply is an electrical system or mechanism that provides emergency power when the main power source fails.[18] They are typically used to protect devices, data centers, and telecommunication equipment if an unexpected disruption could cause injuries, fatalities, significant business disruptions, or loss of data or information. Without operational uninterruptible power supplies, equipment will not function during power fluctuations or outages, resulting in interruption of data flow and disruption of access to network resources.

During the site visit, the inspection team found

- 78 percent (42 of 54) of the communication closets had uninterruptible power supplies that were not plugged into outlets identified as being connected to emergency power,[19] and
- 6 percent (3 of 54) of communication closets were missing uninterruptible power supplies and did not have outlets identified as being connected to emergency power.

Environmental Controls

The team found the equipment was not grounded in about 93 percent of the communication closets, and VA policy requires equipment in communication closets to be properly grounded.[20] Facility staff were unaware of this policy requirement. Without proper grounding, the equipment may not function correctly because of increased electromagnetic interference and power surges.

What the OIG Recommended

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

1. Obtain an inventory of locally managed databases, perform configuration compliance scans, provide the facility with a copy of the scan results, and monitor the facility's remediation efforts.

[18] NIST Special Publication 800-53.

[19] In the event of a prolonged power outage, the uninterruptible power supplies would not be able to support the equipment.

[20] OIT's Infrastructure Standard for Telecommunications Spaces, v3.1 July 2021.

2. Implement a process to verify system owners review user account access to locally managed databases.
3. Implement effective system life-cycle processes to ensure network devices meet standards mandated by the VA Office of Information and Technology Configuration Control Board.
4. Develop and approve an authorization to operate for the special-purpose systems.
5. Include system personnel during the security categorization process to ensure that all necessary information types are considered when determining the security categorization for special-purpose systems.

The OIG made the following recommendations to the VA Bedford Healthcare System director in conjunction with the assistant secretary for information and technology:

6. Implement controls to ensure the accuracy of user locations supporting the Lynx Duress system.
7. Implement the appropriate physical security controls to restrict and monitor access to the facility, its server room, and communication closets.
8. Implement and monitor emergency power and uninterruptible power supplies in all communication closets.
9. Implement grounding equipment in all communication closets.

VA Management Comments and OIG Response

The assistant secretary for information and technology and chief information officer concurred with recommendations 1–9 and submitted planned corrective actions that are responsive to the intent of each recommendation. To support his request that recommendations 2 and 3 be closed, the assistant secretary provided sufficient evidence showing that the actions taken in response to these recommendations have been completed. Therefore, the OIG considers these recommendations closed. The OIG will monitor implementation of the planned actions and will close the remaining recommendations when VA provides evidence demonstrating progress in addressing the identified issues.

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
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

Introduction

Information security controls protect VA systems and data from unauthorized access, use, modification, or 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.[21] The FISMA audit is conducted in accordance with guidelines issued by the Office of Management and Budget and applicable National Institute of Standards and Technology (NIST) information security guidelines.[22] Appendix A details the audit's recommendations. In 2020, the OIG started an information security inspection program to complement the FISMA audit. These inspections assess whether VA facilities are meeting federal security requirements that protect systems and data from unauthorized access, use, modification, or destruction.[23] They are typically conducted at selected facilities that have not been assessed in the sample for the annual FISMA audit or at facilities that previously performed poorly. Inspections provide recommendations to VA on enhancing information security oversight at local and regional facilities.[24] Appendix C provides more detail on the inspection scope and methodology.

The OIG conducted this inspection to determine whether the Bedford VA Healthcare System was meeting federal security guidance. The OIG selected the Bedford VA 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 Bedford VA Healthcare System, other facilities across VA could benefit from reviewing this information and considering these recommendations.

Security Controls

Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of

[21] Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551–3558.

[22] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2022*, Report No. 22-01576-72, May 17, 2023.

[23] Appendix B presents background information on federal information security requirements.

[24] The OIG provided VA with a memorandum 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, the memorandum is not being published by the OIG or distributed outside of VA to prevent intentional or inadvertent disclosure of specific vulnerabilities or other information that could be exploited to interfere with VA's network operations and adversely affect the agency's ability to accomplish its mission.

the system and its information.[25] Both the Office of Management and Budget and NIST provide criteria to evaluate security controls. These criteria provide requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system.[26]

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. In addition, VA Handbook 6500 describes the risk-based process for selecting system security controls, including the operational requirements.[27] VA established guidance outlining both NIST and VA-specific requirements to help information system owners select the appropriate controls to secure their systems.

The OIG information security inspections are focused on three security control areas that apply to local facilities and have been 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 are at risk of unauthorized access or modifications. A cyberattack could destroy, disrupt access to, or allow malicious control of personal

[25] Committee on National Security Systems, *Committee on National Security Systems (CNSS) Glossary*, CNSSI No. 4009, March 2, 2022.

[26] Office of Management and Budget Circular A-130, app. 3, "Security of Federal Automated Information Resources," July 28, 2016; NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations,* September 23, 2021.

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

information belonging to patients, dependents, beneficiaries, VA employees, contractors, or volunteers.

Office of Information and Technology Structure and Responsibilities

The assistant secretary for information and technology and chief information officer leads the Office of Information and Technology (OIT). According to VA, OIT delivers available, adaptable, secure, and cost-effective technology services to VA and acts as a steward for VA's information technology (IT) assets and resources. 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 emerging and imminent threats and vulnerabilities. OIT's Office of Development, Security, and Operations unifies software development, software operations, service management, information assurance, cybersecurity compliance, performance monitoring, and technical integration throughout the entire solution delivery process.

The Office of Information Security; Cybersecurity Operations Center; Office of Development, Security, and Operations; and End User Operations are the OIT offices relevant to the areas assessed at the VA Bedford Healthcare System, as shown in figure 1.

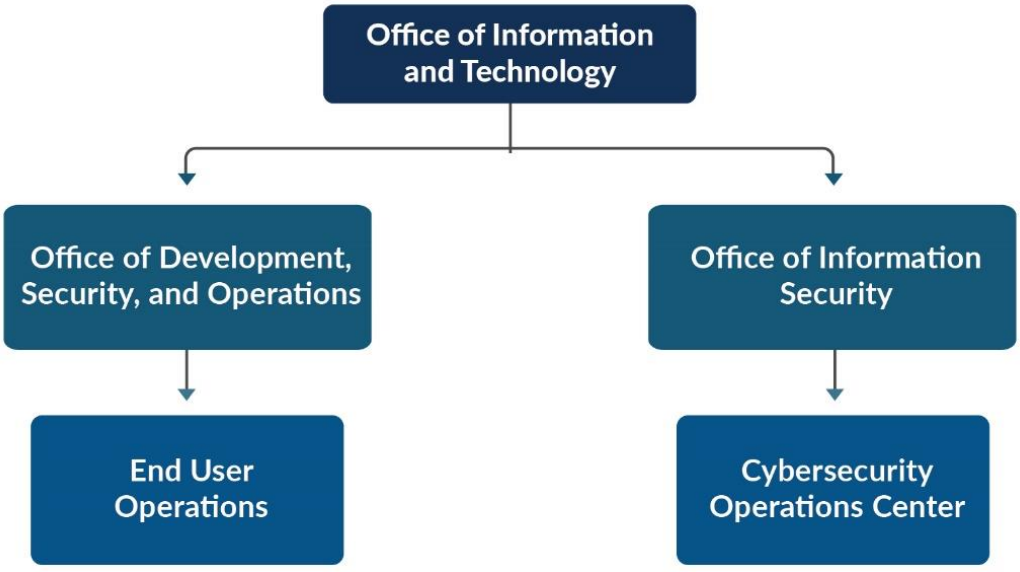

Figure 1. *Organizational structure of Office of Information and Technology entities relevant to this inspection.*

Source: VA OIG analysis.

End User Operations provides on-site and remote support to IT customers across all VA administrations and special program offices, including direct support of approximately 390,000 VA employees and over 100,000 contractors who are issued government-furnished IT equipment and access. End User Operations provides computing devices; conducts new facility activations; performs moves, adds, and changes; executes local system implementations; and

engages VA's customers across the nation to meet IT support needs. OIT assigns dedicated End User Operations and Office of Information Security personnel to the Bedford VA Healthcare System, including system stewards responsible for managing system plans of action and milestones to ensure all assessed and scanned vulnerabilities are documented.

Results of Previous Projects

As previously mentioned, the OIG issues annual reports on VA's information security program. The FISMA audit is conducted in accordance with guidelines issued by the Office of Management and Budget and applicable NIST information security guidelines.[28] The fiscal year (FY) 2022 FISMA audit, conducted by independent public accounting firm CliftonLarsonAllen LLP, evaluated 47 major applications and general support systems hosted at 23 VA facilities, including the testing of selected management, technical, and operational controls outlined by NIST.[29] CliftonLarsonAllen LLP made 26 recommendations, listed in appendix A. All 26 recommendations are repeated from the prior annual audit, indicating that VA continues to face significant challenges in complying with FISMA requirements.[30] Repeat recommendations included addressing deficiencies in configuration management, security management, and access controls.

A statement prepared by the Government Accountability Office (GAO) for a House Veterans' Affairs subcommittee hearing in November 2019 said VA was one of the federal agencies that continued to have a deficient information security program.[31] According to GAO, 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.

[28] Office of Management and Budget Memo M-21-02, "Fiscal Year 2020–2021 Guidance on Federal Information Security and Privacy Management Requirements," November 9, 2020; NIST Special Publication 800-53; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2022*. Appendix A details the FISMA audit's recommendations.

[29] Office of Management and Budget, Circular A-130, app. 3, "Security of Federal Automated Information Resources," November 28, 2000. The circular's appendix defines a general support system as an interconnected set of information resources under the same direct management control which share common functionality.

[30] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2022*. Appendix B presents information about FISMA and other federal criteria and standards discussed in this report.

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

GAO concluded that "until VA adequately mitigates security control deficiencies, the sensitive data maintained on its systems will remain at increased risk of unauthorized modification and disclosure, and the systems will remain at risk of disruption."[32]

VA Bedford Healthcare System

An OIT representative indicated the VA Bedford Healthcare System consists of the Edith Nourse Rogers Memorial Veterans' Hospital, shown in figure 2, and the Gloucester, Haverhill, and Lynn VA clinics. The Edith Nourse Rogers Memorial Veterans' Hospital managed 16,947 unique outpatients in FY 2023. It houses 356 beds, including 238 community living beds and a 51-bed domiciliary for veterans who are experiencing homelessness or at risk of homelessness. The facility has 1,514 full-time employees and a budget of $225 million for FY 2023.

Figure 2. *Edith Nourse Rogers Memorial Veterans' Hospital, Bedford, Massachusetts. Source: Bedford VA Healthcare System; area manager, June 12, 2023.*

[32] GAO, *Information Security.*

Results and Recommendations

I. Configuration Management Controls

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 life cycle.[33] The inspection team reviewed and evaluated 12 configuration management controls drawn from NIST criteria for VA-hosted systems at the VA Bedford Healthcare System to determine if the controls met federal guidance and VA requirements.

An effective configuration management process should be described in a configuration management plan and implemented according to the plan.[34] OIT's Cybersecurity Operations Center identifies and reports on threats and vulnerabilities. Vulnerabilities that cannot be remediated by OIT's Enterprise Vulnerability Management are assigned to system personnel or the information security officer for action. This process helps to secure devices from attack.

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

To assess configuration management controls, the inspection team interviewed the area manager, information system security officer, and local IT specialists. The team reviewed local policies, procedures, and inventory lists and scanned the VA Bedford Healthcare System's network to identify devices. The team compared the devices found on the network with the device inventories provided by VA, received vulnerability lists provided by OIT, and scanned the network to identify vulnerabilities and compliance with baseline configurations.[35] The team also conducted a walk-through of the facility.

The Bedford VA Healthcare System had a deficiency in configuration monitoring, which is the process by which the organization monitors the baseline and operational configuration of hardware, software, and firmware. Specifically, analysis of the OIT vulnerability scan results indicated that the healthcare system's databases were not scanned for compliance with approved baseline configurations, did not meet the established baseline configurations, and were not monitored for administrative user access to the databases. Further, the OIG team found a

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

[34] GAO, *FISCAM*.

[35] OIT imports its vulnerability scan results into the Information Central Analytics and Metrics Platform for reporting vulnerabilities to system owners. See appendix C for additional information about the inspection's scope and methodology.

deficiency in the System Life-Cycle Management, which is how organizations update software on a timely basis to guard against known vulnerabilities.[36] Specifically, the healthcare system's network devices were running outdated software, including software that was no longer supported by the vendor.

Database Configuration Monitoring

The inspection team identified 10 instances in which databases hosting personally identifiable information were not monitored with quarterly compliance scans to detect unresolved security issues. While an OIT representative indicated the database servers were reimaged within the last six months, without quarterly compliance scans, management has no assurance that these databases are configured in compliance with VA configuration security baselines. The inspection team evaluated the servers and found approximately 67 percent of the databases did not meet VA's configuration baselines because they were not scanned for vulnerabilities and were not configured to capture audit logs. OIT representatives stated that it is the responsibility of healthcare system personnel to request compliance scans for databases owned and maintained by the facility or their contractors. The healthcare system personnel did not request these databases to be scanned because they believed that the computers were recently reimaged and maintained by a contractor, therefore there was no need to have the databases scanned for compliance. Regardless, unless the databases are scanned for compliance with approved security baselines, VA does not know whether the databases are securely configured. Also, user account access to these databases was not monitored for unauthorized access. The facility could not provide evidence that audit logs for these databases were captured. Without effective database monitoring, there is an increased risk that a data breach of personally identifiable information could occur and go undetected.

System Life-Cycle Management

The inspection team noted about 87 percent of the healthcare system's network devices used operating systems that did not meet baseline security requirements. More importantly, 4 percent (four devices) were at the end of their useful life and no longer received operating system software maintenance support from the vendor.[37] The OIG identified 12 vulnerabilities, spread over the four network devices, that were acknowledged by the Cybersecurity and Infrastructure Security Agency as known exploited vulnerabilities that need to be remediated by all federal civilian executive branch agencies.[38] The facility's IT staff pointed out that the outdated software

[36] NIST Special Publication 800-53.

[37] The network device vendor announced the end-of-life on January 31, 2022.

[38] This remediation mandate is in accordance with Department of Homeland Security, Binding Operational Directive 22-01, *Reducing Significant Risk of Known Exploited Vulnerabilities*, dated November 3, 2021.

was allowed based on VA procedure; however, the OIG disagrees, as VA policy states, "Do not use unsupported EOL [end of life] software," as a best practice.[39]

In accordance with VA policy, these network devices should have been updated with vendor-supported systems as part of the standard system development life-cycle process. Specifically, baseline configurations should be documented, formally reviewed, and reflect management's agreed-upon system specifications and configurations for those systems. Baseline configurations serve as a basis for future changes to systems that include security and privacy control implementation.[40] The baseline configurations for the network equipment are established by the VA OIT Configuration Control Board. Network devices and IT systems are an organization's most critical infrastructure. Upgrading is not just a defensive strategy but a proactive one that helps protect network stability.

Finding 1 Conclusion

Facility databases did not adhere to established baseline configurations, and databases were not monitored for compliance with VA security policy. Further, network devices were using outdated software that was no longer supported by the vendor. Without effective configuration management controls, management does not have adequate assurance that the system and network will perform as intended and to the extent needed to support their missions.

Recommendations 1–3

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

1. Obtain an inventory of locally managed databases, perform configuration compliance scans, provide the facility with a copy of the scan results, and monitor the facility's remediation efforts.
2. Implement a process to verify system owners review user account access to locally managed databases.
3. Implement a more effective system life-cycle process to ensure network devices meet standards mandated by the VA Office of Information and Technology Configuration Control Board.

[39] Local Area Network (LAN Security Configuration Baseline, version 1.0, September 28, 2021. Vulnerability Management End of Life Policy, June 13, 2023.

[40] NIST Special Publication 800-53.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 1–3 and requested recommendations 2 and 3 be closed due to corrective actions he said were completed. For recommendation 1, the assistant secretary stated VA will enter tickets into the IT service management tool to remediate issues identified in the database scans. Regarding recommendations 2 and 3, the assistant secretary reported VA has completed all database training in connection with standard security reviews and, as of December 2023, has updated all network devices to approved operating systems. The full text of the assistant secretary's response is included in appendix D.

OIG Response

For recommendations 1–3, the planned corrective actions are responsive to the intent of the recommendations. The assistant secretary provided sufficient evidence to support actions taken in response to recommendations 2 and 3 were completed, and the OIG considers these recommendations closed. The OIG will monitor implementation of the planned actions and will close the open recommendation when VA provides evidence demonstrating progress in addressing the issues identified.

II. Security Management Controls

According to *FISCAM*, security management controls establish a framework and continuous cycle for assessing risk, developing security procedures, and monitoring the effectiveness of the procedures. The inspection team evaluated three critical elements of security management: authorization to operate, security categorization, and continuous monitoring of systems.

Finding 2: The VA Bedford Healthcare System Had Deficiencies in Three Security Management Controls

To assess security management controls, the inspection team reviewed local security management policies, standard operating procedures, and applicable VA policies, including documentation from the Enterprise Mission Assurance Support Service—VA's cybersecurity management service for workflow automation and continuous monitoring. Among the documents reviewed were the system security plan, security authorization and risk assessment, security control policies and procedures, and plans of action and milestones for known deficiencies. The team also interviewed the area manager and information system security officer. Finally, the team conducted a walk-through of the facility. The OIG identified three security management control weaknesses at the VA Bedford Healthcare System: authorization to operate, security categorization, and continuous monitoring of the Lynx Duress panic button system.[41]

Authorization to Operate

Regarding system security authorizations, the inspection team found that the facility's special-purpose systems did not have an authorization to operate as required by policy.[42] Furthermore, these special-purpose systems were assigned a moderate risk security categorization without consideration of higher risk information types included in the systems. According to guidance, OIT issues an authorization to operate an information system and explicitly accepts the risk to agency operations, assets, individuals, or other organizations based on the implementation of approved security and privacy controls.[43] The inspection team determined that the facility's special-purpose systems did not have an authorization to operate

[41] The security categorization indicates the minimum baseline controls needed to secure the system. *FISCAM* critical elements for security management are listed in appendix B. The Lynx Duress system is a panic button system that sends a silent alarm to VA's local facility police alerting them if there is an emergency situation requiring their immediate attention.

[42] Office of Management and Budget Circular A-130; VA Directive 6500.

[43] Office of Management and Budget Circular A-130, app. 2.

because they had not cleared the NIST risk management framework.[44] The special-purpose systems included systems "that assist, support, and maintain mission capabilities and operations for building safety, healthcare services, security services, and other general services functional support areas."[45]

Without an authorization to operate, facility managers do not have assurance that the implemented security and privacy controls reduce the risk of a system compromise to an acceptable level. A compromise of a special-purpose system's security could threaten the safety of patients, staff members, and visitors.

Security Categorization

The VA Bedford Healthcare System had authorization boundaries for special-purpose systems for which OIT completed a consolidated security categorization; however, when completing the consolidated security categorization, OIT did not consider all information types when establishing the security category level. The OIG previously identified this issue during the information security inspection of the VA Beckley Healthcare System in West Virginia.[46] NIST's risk management framework requires the baseline controls for information systems to be set based on the needs for confidentiality, integrity, and availability of the information within each system.[47] Minimum security category settings—low, medium, or high—are used when determining baseline controls.[48]

OIT used a single standard for all special-purpose systems, and the security categorization only included the "general information" type. As a result, managers assigned those special-purpose systems a security risk categorization of low for confidentiality, moderate for integrity, and moderate for availability. However, the inspection team determined that the healthcare system's special-purpose systems included a panic button system that warranted higher security levels. The network panic button system falls under the "emergency-response information" type and should have a security categorization of low for confidentiality, high for integrity, and high for availability, as recommended by NIST.[49]

---

[44] The NIST risk management framework integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle. Managing organizational risk is paramount to effective information security and privacy programs.

[45] VA's Enterprise Mission Assurance Support Service.

[46] VA OIG, *Information Security Inspection at the VA Beckley Healthcare System in West Virginia,* Report No. 23-00089-144 September 21, 2023.

[47] NIST Special Publication 800-53B, *Control Baselines for Information Systems and Organizations,* October 2020.

[48] NIST Special Publication 800-60, vol.1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.

[49] NIST Special Publication 800-60, vol. 2, *Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices*, August 2008.

Although NIST allows the security categorization to be adjusted, OIT would need to document the rationale or justification for any adjustments, which was not done. Furthermore, the VA Bedford Healthcare System's special-purpose system security plan only considers security controls based on the lower security categorization developed by OIT. By not considering all information types during the security categorization, healthcare system leaders do not have assurance that appropriate security and privacy controls have been selected for special-purpose systems at their facility.

Continuous Monitoring of Lynx Duress System

The inspection team determined that improvements are needed for monitoring user locations within the Lynx Duress panic button system. The panic button is run by software on the user's laptop and is triggered by pushing both F9 and F11 keys at the same time. VA's domain infrastructure division chief stated that local OIT personnel once maintained the user location information for the panic button system; however, a change during the early months of the COVID-19 pandemic allowed individuals to work at different locations within the hospital. As a result, users are required to enter their location information into their workstations when they log on at a new location.

A VA police representative stated that users ignore prompts to enter location information. When users enter their location information, the user is also flagged to run a test to verify the location. Within the past year, only about 60 to 74 percent of users had completed monthly automated tests of the systems to ensure accurate location information. Additionally, there is no central repository of location information within the system to determine whether the information was entered other than the user test. In the event the location information is not included, police response to a triggered panic button could be delayed and result in life-threatening injuries to employees or patients.

Finding 2 Conclusion

The facility's special-purpose IT system did not have an authorization to operate. Further, OIT did not consider all information types when performing risk assessments of similar systems at 137 VA healthcare systems. Consequently, managers created a single security category for all special-purpose systems that did not have an authorization to operate. Finally, controls are needed to ensure that VA's Lynx Duress panic button system has accurate user location information. Without effective security management processes, management does not have adequate assurance that their IT systems and networks will perform as intended and to the extent needed to support VA missions.

Recommendations 4–6

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

4. Develop and approve an authorization to operate for the special-purpose systems.
5. Include system personnel during the security categorization process to ensure that all necessary information types are considered when determining the security categorization for special-purpose systems.

The OIG made one recommendation to the VA Bedford Healthcare System director in conjunction with the assistant secretary for information and technology:

6. Implement controls to ensure the accuracy of user locations contained within the Lynx Duress system.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 4–6. For recommendation 4, the assistant secretary stated VA is applying the approved assessment and authorization process for special-purpose systems. The assistant secretary also reported that, in response to recommendation 5, VA is performing additional security analysis on systems and updating the Enterprise Risk Analysis process to include language that documents the appropriate language highlighted by the OIG. Regarding recommendation 6, the assistant secretary stated VA is developing guidance and training that will be driven by each service line chief to ensure employees continue to provide proper location updates within Lynx Duress system. The full text of the assistant secretary's response is included in appendix D.

OIG Response

For recommendations 4–6, the planned corrective actions are responsive to the intent of the recommendations. The OIG will monitor implementation of the planned actions and will close the open recommendations when VA provides evidence demonstrating progress in addressing the issues identified.

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.[50] 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 actions users can take. Physical access controls involve restricting physical access to computer resources and protecting them from loss or impairment. Identification, authentication, and authorization controls ensure that users have the proper access, and that access is restricted to authorized individuals. At the Edith Nourse Rogers Memorial Veterans' Hospital, the main facility within the VA Bedford Healthcare System, the inspection team reviewed two critical access control elements: access controls and environmental controls.[51]

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

To evaluate access controls on the VA Bedford Healthcare System's network, the inspection team reviewed the configuration of network equipment and interviewed the area manager, information system security officer, biomedical supervisor, and local IT specialists. The team also reviewed local policies and procedures, conducted walk-throughs of the facility, and analyzed audit logs.[52]

The VA Bedford Healthcare System's server room and communication closets did not have adequate physical and environmental controls.[53] Specifically, the team noted the following:

- Physical access to the hospital, the server room, and communication closets was not adequately restricted.
- Access to the server room and communication closets was not adequately monitored.
- Emergency power and uninterruptible power supplies were not implemented or not connected to emergency power sources in all communication closets.
- Electrical grounding was not implemented in all communication closets.

[50] Boundary protections include access control lists that restrict the flow of network traffic between network segments.

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

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

[53] Environmental controls include electrical grounding, fire protection, and temperature and humidity controls.

Physical Access Controls

The inspection team discovered that physical access to the hospital 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.[54] The facility had an automated system that required badges to enter the server room. The team found badges assigned to 39 individuals who should not have had access to the server room were granted the ability to enter it. These 39 individuals included 10 former employees.[55] Further, employees were assigned keys to access communication closets because badge readers were not functioning to restrict and record physical access to the communication closets. No plan of action and milestones had been created to address the faulty proximity card devices until after the OIG announced it would conduct an information security inspection. To compensate, facility personnel depended on key access to the communication closets. Further, the process controls over key inventory were inadequate. For example, an inventory of master keys had not been conducted since 2009. Since this issue was identified, the master key inventory was reduced from 41 to 27 keys.

Monitoring of Access to the Server Room and Communication Closets

The hospital did not have adequate controls to monitor access to the server room and communication closets. Specifically, the electronic badging access system allows monitoring of the server room; however, it does not monitor access to the communication closets. During the facility walk-through, the inspection team also discovered that the medical center did not have a comprehensive video surveillance system; specifically, the video surveillance system did not monitor access to the server room or communication closets. Video surveillance is required for server rooms.[56] Ineffective monitoring of access to server rooms and communication closets minimizes the facility's incident response capabilities in the event of a security compromise. The lack of an effective incident response can undermine managers' awareness of security vulnerabilities that could hinder the operation of mission critical systems.

Emergency Power Controls

The facility server room and communication closets did not meet federal and VA environmental security requirements. At the facility, the team found

[54] NIST Special Publication 800-53.

[55] OIT indicated that badges are collected when employees are terminated, and the individuals with access did not use it.

[56] NIST Special Publication 800-53.

- 78 percent (42 of 54) of the communication closets had uninterruptible power supplies that were not plugged into power outlets identified as being connected to an emergency power supply, and[57]
- 6 percent (3 of 54) of the communication closets were missing uninterruptible power supplies and did not have power outlets identified as being connected to an emergency power supply.

Uninterruptible power supplies are electrical systems or mechanisms that provide emergency power when the main power source fails.[58] They are typically used to protect devices and telecommunications equipment if an unexpected disruption could cause injuries, fatalities, business disruption, or loss of data or information. Uninterruptible power supplies differ from emergency power systems for backup generators because they provide near-instantaneous protection from interruptions. Without operational uninterruptible power supplies, equipment will not function during power fluctuations or outages, resulting in interruption of data flow and disruption of access to network resources.

Environmental Controls

The team found equipment that was not grounded in approximately 93 percent of the communication closets. VA policy requires this equipment to be properly grounded.[59] Facility personnel were unaware of this issue.[60] Without proper grounding, the equipment could be damaged by electromagnetic interference and power surges.

Finding 3 Conclusion

The VA Bedford Healthcare System's server room and communication closets did not have adequate physical and environmental controls. Specifically, physical access to the server room and communication closets was not adequately restricted or monitored for unauthorized access. Emergency power and uninterruptible power supplies were not implemented or properly functioning in the communication closets. Finally, electrical grounding controls were not implemented in all communication closets to prevent power surges. Unless the healthcare system takes corrective actions, it risks unauthorized access to critical network resources, inability to respond effectively to incidents, and potentially the loss of personally identifiable information.

[57] In the event of a prolonged power outage, the uninterruptible power supplies would not be able to support the equipment.

[58] NIST Special Publication 800-53.

[59] OIT's Infrastructure Standard for Telecommunications Spaces, v3.1 July 2021.

[60] NIST Special Publication 800-53; VA Telecommunications and Special Telecommunications Systems Design Manual, February 2016.

Recommendations 7–9

The OIG made three recommendations to the VA Bedford Healthcare System director in conjunction with the assistant secretary for information and technology:

7. Implement the appropriate physical security controls to restrict and monitor access to the facility server room and communication closets.
8. Implement emergency power and uninterruptible power supplies in all communication closets.
9. Implement electrical grounding equipment in all communication closets.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 7–9. For recommendation 7, the assistant secretary stated VA is implementing a plan to restrict and monitor access to the facility server room and communication closets. Regarding recommendations 8 and 9, the assistant secretary reported that VA has ordered uninterruptible power supplies to be installed in all communication closets that do not have one installed, and stated VA will install electrical equipment grounding as part of the Electronic Health Record Modernization infrastructure upgrades project. The full text of the assistant secretary's response is included in appendix D.

OIG Response

For recommendations 7–9, the planned corrective actions are responsive to the intent of the recommendations. The OIG will monitor implementation of the planned actions and will close the open recommendations when VA provides evidence demonstrating progress in addressing the issues identified.

Appendix A: FISMA Audit for FY 2022 Report Recommendations

In the Federal Information Security Modernization Act of 2014 (FISMA) audit for FY 2022, CliftonLarsonAllen LLP made 26 recommendations, all repeated from the prior year. The FISMA audit assesses the agency-wide security management program, and recommendations in the FISMA report are not specific to the Bedford VA Healthcare System. The 26 recommendations are listed below:

1. Consistently implement an improved continuous monitoring program in accordance with the National Institute of Standards and Technology 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.
7. Implement periodic reviews to minimize access by system users with incompatible roles, permissions in excess of required functional responsibilities, and unauthorized 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 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 a more effective patch and vulnerability management program to address security deficiencies identified during our assessments of VA's web applications, database platforms, network infrastructure, and workstations.
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 network access controls that restrict medical devices from systems hosted on 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.[61]
17. Implement improved procedures to enforce standardized system development and change control processes that integrate information security throughout the life cycle of each system.
18. Review system boundaries, recovery priorities, system components, and system interdependencies and implement appropriate mechanisms to ensure that established system recovery objectives can be measured and met.
19. Ensure that contingency plans for all systems are updated to include critical inventory components and are tested in accordance with VA requirements.
20. Implement more effective agency-wide incident response procedures to ensure timely notification, reporting, updating, and resolution of computer security incidents in accordance with VA standards.
21. Ensure that systems and applications are adequately logged and monitored to facilitate an agency-wide awareness of information security events.

[61] Credentialed vulnerability assessments are vulnerability scans performed using a user account and password.

22. Implement improved safeguards to identify and prevent unauthorized vulnerability scans on VA networks.
23. 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 action and milestones.
24. Implement improved processes to monitor for unauthorized changes to system components and the installation of prohibited software on all agency devices and platforms.
25. Develop a comprehensive inventory process to identify connected hardware, software, and firmware used to support VA programs and operations.
26. 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 provide auditors and information system control specialists a specific methodology for evaluating the confidentiality, integrity, and availability of information systems.[62] *FISCAM* groups related controls into categories that have similar risks. To assist auditors in evaluating information systems, *FISCAM* maps control categories to 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 management's 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.[63] Products should comply with applicable standards and the vendors' good security practices. The organization should have the ability to monitor and test to determine if a system is functioning as intended, as well as to determine if networks are appropriately configured and paths are protected between information systems.
- **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

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

[63] Firmware are computer programs and data stored in hardware, typically in read-only memory, that cannot be written or modified during the execution of the program.

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 personnel 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, due to the increased risk of errors, emergency changes should be kept to a minimum.

FISCAM identifies the following critical elements for contingency planning:

- **Computerized operations criticality and sensitivity assessment** is an analysis of data and operations by management to determine which are the most critical and what resources and 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 for 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.

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 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 that 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 management.
- **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 that 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.

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.

Federal Information Security Modernization Act of 2014

The stated goals of FISMA are:

- Provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.
- Recognize the highly networked nature of the current federal computing environment and provide effective government-wide management and oversight of the related information security risks.
- Provide for development and maintenance of minimum controls required to protect federal information and information systems.
- Provide a mechanism for improved oversight of federal agency information security programs.
- Acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions.
- Recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.[64]

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

[64] Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551–3558.

conduct annual evaluations. The OIG accomplishes the annual FISMA evaluation through a contracted external auditor and provides oversight of the contractor's performance.

NIST Information Security Guidelines

The Joint Task Force Transformation Initiative Working Group created the NIST information security guidelines.

Appendix C: Scope and Methodology

Scope

The inspection team conducted its work from May 2023 through January 2024. The team evaluated configuration management, security management, and access controls of operational VA information technology (IT) assets and resources in accordance with FISMA, NIST security guidelines, and VA's IT security policy. In addition, the team assessed the capabilities and effectiveness of IT security controls used to protect VA systems and data from unauthorized access, use, modification, and destruction.

Methodology

To accomplish the objective, the inspection team examined relevant laws and policies and inspected the center and systems for security compliance. Additionally, the team interviewed VA personnel responsible for the Bedford VA Healthcare System's IT security, operations, and privacy compliance. 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 that 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 GAO's *FISCAM* as a template to plan for the inspection. When planning for this review, the team identified potential information system controls that would significantly affect the review. Specifically, the team used the *FISCAM* appendix 2 as a guide to help develop evidence requests and interview questions for healthcare system personnel. The team used the *FISCAM* controls identified in appendix B of this report to determine the FISMA controls used by VA to protect and secure its information systems. Although similar to the contractor-conducted annual FISMA audits, this review focused on security controls that are implemented at the local level. However, there are some controls that 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 that all controls applicable to the Bedford VA Healthcare System are 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.

Fraud Assessment

The inspection team assessed the risk that fraud and noncompliance with provisions of laws, regulations, contracts, and grant agreements, significant in the context of the audit objectives, could occur during this inspection. The team exercised due diligence in staying alert to any fraud indicators. The OIG did not identify any instances of fraud or potential fraud during this inspection.

Data Reliability

The inspection team generated computer-processed data by using network scanning tools. The results of the scans were provided to the OIT Quality Performance and Risk team. The team used industry-standard information system security tools to identify information systems on the VA network and to take snapshots of their configurations, which were used to identify vulnerabilities. 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.

Government Standards

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

Appendix D: VA Management Comments

Department of Veterans Affairs Memorandum

Date: March 22, 2024

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

Subj: Information Security Inspection of the VA Bedford Healthcare System in Massachusetts, Project Number 2023-02330-AE-0086 (VIEWS 11450067)

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, *Information Security Inspection of the VA Bedford Healthcare System in Massachusetts* (Project Number 2023-02330-AE-0086).

2. The Office of Information and Technology (OIT) submits the attached written comments, along with a target completion date or closure evidence for each of the OIG's recommendations to the Department.

The OIG removed point of contact information prior to publication.

(Original signed by)

Kurt D. DelBene

Attachment

Attachment

Office of Information and Technology

Comments on Office of Inspector General Draft Report,

Information Security Inspection of the VA Bedford Healthcare System in Massachusetts,

Project Number OIG-2023-02330-AE-0086

(VIEWS 11450067)

Recommendation 1: Obtain an inventory of locally managed databases, performed configuration compliance scans, provide the facility with a copy of the scan results, and monitor the facilities' remediation efforts.

Comments: Concur.

The Department of Veterans Affairs (VA) will enter tickets in the information technology service management tool for remediation assistance on issues identified in the database scans. The Bedford Healthcare System is coordinating and collaborating with the Office of Information and Technology (OIT) to make contingency systems available for continuous use.

Expected Completion Date: June 30, 2024.

Recommendation 2: Implement a process to verify system owners review user account access to locally managed databases.

Comments: Concur.

VA has completed all required database training that falls under standard security reviews. Once an administrative session begins, the session is recorded as shown in the screenshot provided to the Office of Inspector General (OIG) inspection team. VA manages and maintains records of all actions taken while connected through the session.

Expected Completion Date: Completed. Completion date: January 29, 2024.

VA requests closure of Recommendation 2.

Recommendation 3: Implement a more effective system life cycle process to ensure network devices meet standards mandated by the VA Office of Information and Technology Configuration Control Board.

Comments: Concur.

VA updated the Operating System (OS) version on all network devices at the Bedford Healthcare System to a VA-approved version on December 12, 2023. An email was provided to the OIG inspection team with the current OS version to verify the upgrade as requested.

Expected Completion Date: Completed. Completion date: December 12, 2023.

VA requests closure of Recommendation 3.

Recommendation 4: Develop and approve an authorization to operate for the special-purpose systems.

Comments: Concur.

VA is applying the approved assessment and authorization process for special-purpose systems (SPS). SPS security plans and boundaries will be assessed for an authorization to operate by a VA authorizing official. The roadmap development has an expected completion date of June 28, 2024.

Expected Completion Date: June 28, 2024.

Recommendation 5: Include system personnel during the security categorization process to ensure that all necessary information types are considered when determining the security categorization for special-purpose systems.

Comments: Concur.

VA is performing additional security analysis on systems and updating the Enterprise Risk Analysis to include language that documents the baseline risk score HIGH and appropriate language highlighted by the OIG.

Expected Completion Date: April 30, 2024.

Recommendation 6: Implement controls to ensure the accuracy of user locations contained within the Lynx Duress system.

Comments: Concur.

VA is developing guidance and training that will be driven by each service line chief to ensure employees continue to provide proper location updates within Lynx. Following completion of training, and monthly thereafter, the security specialist will brief the Healthcare Operations Committee on Lynx status.

Expected Completion Date: April 30, 2024.

Recommendation 7: Implement the appropriate physical security controls to restrict and monitor access to the facility server room and communication closets.

Comments: Concur.

VA is implementing a plan to restrict and monitor access to the facility server room and communication closets. VA Police Services will monitor access to all reports of personnel gains and losses to ensure VA access policies are followed.

Expected Completion Date: November 30, 2025.

Recommendation 8: Implement emergency power and uninterruptible power supplies in all communication closets.

Comments: Concur.

VA ordered Uninterruptible Power Supplies (UPS) to be installed in all OIT closets that do not have one installed. Additionally, VA issued a work order to replace all non-compatible UPS.

Expected Completion Date: September 30, 2024.

Recommendation 9: Implement electrical grounding equipment in all communication closets.

Comments: Concur.

VA will install electrical equipment grounding as part of the Electronic Health Record Modernization infrastructure upgrades project.

Expected Completion Date: November 30, 2025.

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 Luis Alicea Keith Hargrove Timothy Moorehead Albert Schmidt Justin Skeen Brandon Zahn
Other Contributors	Charles Hoskinson Clifford Stoddard

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, Bedford VA 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 Accountability
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: Ed Markey, Elizabeth Warren
US House of Representatives: Jake Auchincloss, Katherine Clark, William R. Keating, Stephen Lynch, James McGovern, Seth Moulton, Richard Neal, Ayanna Pressley, Lori Trahan

OIG reports are available at www.vaoig.gov.