US DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS HEALTH ADMINISTRATION

Information Security Inspection at the VA Beckley Healthcare System in West Virginia

Information Security Inspection	**23-00089-144**	**September 21, 2023**

BE A

VOICE FOR VETERANS

REPORT WRONGDOING

va.gov/oig/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, 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 resulted in 26 recommendations made to VA. Repeat recommendations included addressing deficiencies in configuration management, contingency planning, security management, and access controls. 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 the OIG determined to be at highest risk. Typically, facilities selected for these inspections either were not included in the annual FISMA 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 VA Beckley Healthcare System in West Virginia was meeting federal security guidance. The OIG selected the facility because it had not been previously 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 three security control areas: configuration management controls, security management controls, and access controls.[3] Although the findings and recommendations in this report are specific to the VA Beckley Healthcare System, other healthcare systems across VA could benefit from reviewing this information and considering these recommendations.

[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. Appendix A lists the recommendations from the fiscal year 2022 FISMA audit, the most recent audit at the time of this inspection.

[3] 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.

What the Inspection Found

The OIG identified security deficiencies with configuration management, security management, and access controls.

Configuration Management Controls Had Two Deficiencies

Configuration management controls identify and manage security features for all hardware and software components of an information system.[4] The two deficiencies the OIG found in this control area at the VA Beckley Healthcare System involved vulnerability management and flaw remediation.

Prior FISMA audits have repeatedly found deficiencies in VA's vulnerability management, which is the process by which the Office of Information and Technology (OIT) identifies, classifies, and reduces weaknesses. OIT scans for vulnerabilities both routinely and randomly, or when new vulnerabilities are identified, and uses the Information Central Analytics and Metrics Platform (ICAMP) to report vulnerabilities to facilities for remediation. The OIG team found that the information within ICAMP was not complete and accurate. For example, the October ICAMP report contains 22,993 entries for high, critical, and medium host vulnerabilities. However, the team also found that

- 4,813 entries did not include a host name, as they did not have an appropriate domain name system entry,[5]
- 3,783 entries that had a host name did not have a corresponding machine name, and
- 2,280 entries had a different domain name system name from the machine name.[6]

Not having complete and accurate information in the ICAMP vulnerability reports can make it difficult for the healthcare system to remediate vulnerabilities. Further, inaccurate information may skew the results. For example, the October report indicated that a machine had a vulnerability for 103 months on the VA network, despite the machine being on the network for less than 12 months.

To address flaw remediation the inspection team reviewed 13 months of scans of VA vulnerabilities, from November 2021 through November 2022. Based on these scan results, the team identified

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

[5] A host name is the name of a device that the network associates to a given IP address.

[6] The machine name is the name provided to the computer in its configuration.

- 444 high vulnerabilities on about 36 percent of computers that were remediated after the 60-day deadline,
- 405 critical vulnerabilities on about 15 percent of computers that were remediated after the 30-day deadline,
- 218 high vulnerabilities on about 35 percent of computers that were not remediated and were past the 60-day deadline for remediation, and
- 134 critical vulnerabilities on about 20 percent of computers that were not remediated and were past the 30-day deadline for remediation.

Without an effective vulnerability management program, vulnerabilities such as security and functionality problems in software and firmware might not be mitigated, increasing opportunities for exploitation.

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 the procedures."[7] The OIG identified three security management control weaknesses at the VA Beckley Healthcare System: authorization to operate, security categorization, and continuous monitoring.

OIT issues the authorization to operate an information system and explicitly accepts the risk to agency operations, assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security and privacy controls.[8] The OIG determined that the healthcare system's special-purpose information technology (IT) system did not have an authorization to operate because it had not cleared the NIST risk management framework.[9] The special-purpose system included subsystems that monitor the distribution of oxygen throughout the hospital, alert facility police of emergencies via panic buttons, limit access to the control room, and control the facility's climate.

[7] GAO, *FISCAM*.

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

[9] 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.

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 that could threaten the safety of patients, staff members, and visitors.

When examining the special-purpose system at Beckley, the OIG also found that OIT did not consider all information types while establishing security category levels for similar systems at 137 Veterans Health Administration (VHA) facilities. NIST's risk management framework requires the baseline controls for information systems be set based on the needs for confidentiality, integrity, and availability of the information within each system. NIST allows the security categorization to be adjusted but requires the rationale or justification for the adjustment to be documented. OIT did not provide documentation for the justification of any adjustment.

By not considering all information types during the security categorization, VHA healthcare system leaders do not have assurance that appropriate security and privacy controls were selected for special-purpose systems at their facilities to reduce the risk of compromise to an acceptable level.

During the inspection, the OIG also discovered that plans of action and milestones were not created for 18 controls listed as noncompliant or unassessed in VA's Enterprise Mission Assurance Support Service. A plan of action and milestones would provide directions to implement and assess controls identified in VA's Enterprise Mission Assurance Support Service as being noncompliant or not assessed. Without a plan of action and milestones, the risk presented by the vulnerability cannot be managed and needed resources for remediation may not be available.

Access Controls Had Five Deficiencies

Access controls provide reasonable assurance that computer resources are restricted to authorized individuals. The inspection team found that the VA Beckley Healthcare System had access control deficiencies involving network segmentation controls, and that the Beckley VA Medical Center had access control deficiencies with uninterrupted power, physical access controls, environmental controls, and media sanitization.

Network Segmentation Controls

The VA Beckley Healthcare System did not have network segmentation controls in place for several network medical and special-purpose system segments.[10] Network-connected

[10] A special-purpose system segment is a nonmedical, network-connected system that supports building safety, security, or environmental controls and cannot obtain a VA-approved baseline configuration due to vendor-controlled system policies, proprietary software, and other system-specific controls and configurations. Examples of special-purpose systems include energy management systems, heating, ventilation, air conditioning, temperature controls, building or facility access controls, and security camera systems.

special-purpose systems are placed on isolated network segments for protection, as they provide critical infrastructure facility support. However, the team identified seven network segments containing 39 special-purpose system devices that did not have access control lists applied.[11] Further, the team noted an additional network segment, which contained 90 Veterans Health Information System Technology Architecture imaging devices, had access control lists applied but the access control lists did not restrict access from the entire VA network. Finally, the VA Beckley Healthcare System's network contained 941 devices that did not fall within a defined network segment used to identify whether access control lists needed to be applied. Without network segmentation controls in place, any user can access these potentially vulnerable medical devices. After the inspection team reported this issue to OIT, OIT provided support and applied appropriate access control lists to the network segments containing the medical devices.

Uninterrupted Power

The OIG determined that during the monthly generator test, the Beckley VA Medical Center loses power for approximately eight to 10 seconds each time the facility switches to and from generator power. The inspection team observed a generator test and determined that not all systems were connected to an existing or functional uninterrupted power supply. Consequently, the team observed the following:

- The emergency room nurses' central monitoring system, while connected to a nonfunctioning universal power supply, was down for under one minute. However, when the system came back online, the team noted that patient monitors were incorrectly sending an audio alarm falsely indicating that they were removed from patients.
- The emergency room X-ray machines went offline and started an audio alarm when the power returned. Emergency room staff needed to contact radiology staff to reset the machines.
- The main phone line for radiology was down for over four minutes.
- The police security cameras were reset and needed to be refocused to provide the necessary views.

The facility sends out an email that warns staff that "all elevators and electrical equipment, such as lights and computers will experience a brief loss of power" at the start and end of the test. Further, the facility sends an email instructing staff that OIT "requests that all computers be logged off before each of these time frames when we experience a brief loss of power." Even so, single points of failure could cause harm to patient care and degrade IT resources. During an actual power outage, the facility effects would be more severe than what is experienced during

[11] Access control lists provide security by limiting the resources that can be accessed within network segments.

the generator test, as the facility personnel would not have taken known precautions. Facility personnel have reported that power lapses have caused at least one issue on the second floor that delayed lab operations and another issue where there was a delay in a patient transfer.

Physical Access Controls

The Beckley VA Medical Center's computer room and 19 communication closets did not meet VA physical requirements. Implementing inadequate physical controls could adversely affect IT operations and patient care. Specifically, the facility's data lines were

- not all labeled,
- not using cable trays for protection,
- intertwined with electrical lines, and
- not directly plugged into patch panels.

Further, managers did not provide support to ensure that the carpeted raised tiles in the computer room would prevent electrical shocks. Finally, the computer room did not have hot and cold aisles that help units pull in cool air to prevent overheating.

The OIG also found the following deficiencies for 19 communication closets supporting the facility, with some having more than one deficiency:

- Eleven were not monitored by cameras.
- Five did not have an open-door alarm.
- Three did not have a backup dead bolt.
- One did not have personal identity verification card access enabled.

Environmental Controls

The OIG also noted that since 2013, there were 24 incidents and repairs of leaks in the computer room or the adjacent telecommunication room. Additionally, the OIG found standing water on the roof, ceiling tiles that were water damaged, and discolored fire retardant where water leaked from pipes exiting the computer room ceiling to the roof. Facility personnel showed the team rolls of plastic in the computer room that could be used to help protect equipment in the event a leak was detected. However, if a leak were to occur when no one was in the computer room, no other controls were in place to prevent water damage to the computer equipment.

Further, the medical center had several deficiencies in IT environmental controls that protect computer resources within communication closets. Of the 19 closets within which the OIG found deficiencies,

- none had a smoke detector,

- 18 did not contain electrical grounding for equipment,
- 13 did not have temperature- and humidity-monitoring controls,
- seven did not have an uninterrupted power supply, and
- five did not have fire suppression systems.

Without these environmental safeguards, organizational assets could be damaged by electrical surges, water, or fire, resulting in financial loss or harm to veterans.

Media Sanitization

The Beckley VA Medical Center was not sanitizing unencrypted hard drives prior to shipping the hard drives out for destruction. According to an OIT employee and corroborated by evidence collected, the facility damaged the hard drives using a method that would not destroy the data. Specifically, the facility personnel damaged the hard drive physical interface, not realizing that the drive could still be repaired and allow access to data contained on the drives. Media protection personnel did not understand that this would not meet VA's media sanitization requirements. Hard drives that are not sanitized can lead to potential leakage of sensitive veteran information stored on media.

What the OIG Recommended

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

1. Implement a process to minimize the Information Central Analytics and Metrics Platform data reliability issues.
2. Improve vulnerability management processes to ensure system changes occur within organization timelines.
3. Develop and approve an authorization to operate for the special-purpose system.
4. 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.
5. Implement improved mechanisms to ensure system stewards are creating plans of action and milestones for all controls that have not been implemented or assessed.
6. Ensure network segmentation controls are applied to all network segments with special-purpose systems.

The OIG also made four recommendations to the VA medical center director:

7. Install uninterruptible power supplies to eliminate single points of electrical failure supporting the facility.
8. Ensure that hot and cold aisles in computer rooms, and electric and data cables are installed in accordance with VA standards.
9. Validate that appropriate physical and environmental security measures are implemented and functioning as intended.
10. Implement media sanitization methods in accordance with VA policy requirements.

VA Comments and OIG Response

The assistant secretary for information and technology and chief information officer concurred with recommendations 1 and 3 through 10. The planned corrective actions are responsive to the intent of these recommendations. The assistant secretary provided evidence to support actions addressing recommendations 1, 5, and 6 were completed, and the OIG considers these recommendations closed.

The assistant secretary did not concur with recommendation 2 and stated that VA could provide evidence of remediation for vulnerabilities persisting beyond established remediation time frames. However, VA did not provide evidence illustrating that remediation efforts at Beckley were successful. VA has implemented a new process to address vulnerability remediation at the facility. The OIG will continue to monitor the remediation of vulnerabilities and the creation of plans of action and milestones for vulnerabilities that cannot be remediated during the information security inspections. Recommendation 2 will be closed when VA can demonstrate that the plan of action and milestones process can effectively mitigate security risks for unremedied security vulnerabilities.

The OIG will monitor implementation of the planned actions and will close the recommendations when VA provides evidence demonstrating progress in addressing the issues identified. The full text of the assistant secretary's response is included in appendix D.

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
FY	fiscal year
GAO	Government Accountability Office
ICAMP	Information Central Analytics and Metrics Platform
IT	information technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information and Technology
OMB	Office of Management and Budget

Introduction

Information security controls protect VA systems and data from unauthorized access, use, modification, or destruction. 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.[12] The FISMA audit is conducted in accordance with guidelines issued by the Office of Management and Budget (OMB) and applicable National Institute of Standards and Technology (NIST) information security guidelines.[13]

In 2020, the OIG also started an information security inspection program. These information security inspections assess whether VA facilities are meeting federal security requirements that protect systems and data from unauthorized access, use, modification, or destruction.[14] 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.[15] Appendix C provides more detail on the inspection scope and methodology.

The OIG conducted this inspection to determine whether the VA Beckley Healthcare System was meeting federal security guidance. The OIG selected this healthcare system because it had not been previously visited as part of the annual FISMA audit. Although the findings and recommendations in this report are specific to the VA Beckley 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

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

[13] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2022*, Report No. 22-01576-72, May 17, 2023. Appendix A lists the recommendations from the fiscal year 2022 FISMA audit, the most recent audit at the time of this inspection.

[14] Appendix B discusses federal information security requirements in further detail.

[15] 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.[16] Both the OMB 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.[17]

Responsibility for developing and maintaining information security policies, procedures, and control techniques lies with the assistant secretary for information and technology, who is also VA's chief information officer. The risk-based process for selecting system security controls, including the operational requirements is detailed in VA policy.[18] VA established guidance outlining both NIST- and VA-specific requirements to help information system owners select the appropriate controls to secure their systems.

OIG information security inspections are focused on three security control areas that apply to local facilities and have been selected based on their levels of risk, as shown in table 1. The OIG previously also evaluated a fourth control area—contingency planning—but found that controls in that area are predominantly managed at the enterprise level and are therefore no longer included in these inspections.

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.

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

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

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

Without these critical controls, VA's systems are at risk of unauthorized access or modifications. A cyberattack could disrupt, destroy, or allow malicious control of personal 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. Figure 1 provides an overview of the relevant entities' organizational structures.

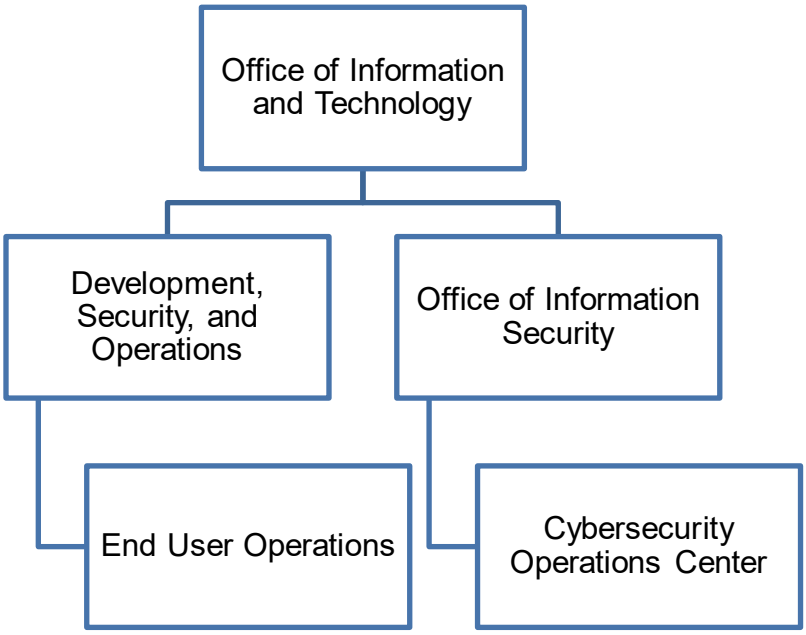

Figure 1. *Organizational structure of OIT entities relevant to this inspection.*
Source: VA OIG analysis.

End User Operations provides onsite and remote support to IT customers across all VA administrations and special program offices, including direct support of over 400,000 VA employees and thousands of contractors who are issued government-furnished IT equipment and access. End User Operations provisions 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 personnel to the VA Beckley Healthcare System, including system stewards who are 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 OMB and applicable NIST information security guidelines.[19] The fiscal year (FY) 2022 FISMA audit, conducted by CliftonLarsonAllen LLP, an independent public accounting firm, evaluated 50 major applications and general support systems hosted at 24 VA facilities, including the testing of selected management, technical, and operational controls outlined by NIST.[20] 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.[21] Repeat recommendations included addressing deficiencies in configuration management, contingency planning, 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.[22] 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

[19] OMB 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, *Security and Privacy Controls for Federal Information Systems and Organizations,* September 23, 2021; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2022*. Appendix A lists the recommendations from the fiscal year 2022 FISMA audit, the most recent audit at the time of this inspection.

[20] OMB, 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.

[21] 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.

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

- managing IT supply chain risks.

GAO concluded that "until VA adequately mitigates security control deficiencies, the sensitive data maintained on its systems will remain at risk of disruption and have an increased risk of unauthorized modification and disclosure, and the system will remain at risk of disruption."[23]

VA Beckley Healthcare System

The VA Beckley Healthcare System consists of the Beckley VA Medical Center and the Princeton and Greenbrier community-based outpatient clinics. The Beckley VA Medical Center saw 12,799 unique outpatients in FY 2022. It also houses 30 general medical care beds and 50 community living center beds.[24] The facility has 963 employees and a budget of $104 million for FY 2023.

Figure 2. *Beckley VA Medical Center.*
Source: VA OIG, taken on November 16, 2022.

[23] GAO, *Information Security: VA and Other Federal Agencies Need to Address Significant Challenges*.
[24] The community living center beds are used for nursing home services provided by VA.

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.[25] The inspection team reviewed and evaluated the 12 configuration management controls drawn from NIST criteria for VA-hosted systems at the VA Beckley Healthcare System to determine if they 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.[26] VA should first establish an accurate component inventory to identify all devices on the network.[27] The component inventory affects the success of other controls, such as vulnerability and patch management. According to the configuration management standard operating procedure, OIT's Cybersecurity Operations Center identifies and reports on threats and vulnerabilities. Vulnerabilities that cannot be remediated by Enterprise Vulnerability Management are assigned to system personnel or the information security officer for action. This process helps to secure devices from attack.[28]

Finding 1: The VA Beckley 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 Beckley 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.[29] A review of the October 2022 vulnerability scan results OIT provided indicated they did not provide healthcare system leaders with complete and accurate information related to vulnerabilities discovered. Further, the vulnerabilities identified were not

[25] *FISCAM*.

[26] *FISCAM*.

[27] *FISCAM*.

[28] VA Directive 6500.

[29] 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.

being remediated by VA's deadlines. Consequently, the inspection team reported issues with vulnerability management and flaw remediation.

Vulnerability Management

VA's vulnerability management program can be improved. Prior FISMA audits repeatedly found deficiencies in VA's vulnerability management controls. Vulnerability management is the process by which OIT identifies, classifies, and reduces weaknesses, and is part of assessing and validating risks as well as monitoring the effectiveness of a security program. The Cybersecurity Operations Center identifies and reports on threats and vulnerabilities, and OIT conducts scans for vulnerabilities both routinely and randomly, or when new vulnerabilities are identified and reported.[30]

VA conducts periodic independent scans of all its systems. To report vulnerabilities to facilities for remediation, the agency uses its Information Central Analytics and Metrics Platform (ICAMP). The inspection team found that the information within ICAMP was not complete and accurate. For example, the October 2022 ICAMP report contained 22,993 entries for high, critical, and medium host vulnerabilities. However, the inspection team found that

- 4,813 entries did not include a host name, as they did not have an appropriate domain name system entry;[31]
- 2,280 entries had a different domain name system name from the machine name; and[32]
- 3,783 entries that had a host name did not have a corresponding machine name.

Not having complete and accurate information in the ICAMP vulnerability reports can make it difficult for the healthcare system to remediate vulnerabilities. Further, inaccurate information may undermine managers' abilities to take appropriate corrective actions. For example, the October report indicated that a machine had a vulnerability for 103 months on the VA network; however, the machine was on the network for less than 12 months.

Flaw Remediation

According to the standard operating procedures, the discovered vulnerabilities are entered into a plan of action and milestones for remediation by the system steward. The system technicians

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

[31] A host name is the name of a device that the network associates to a given IP address.

[32] The machine name is the name provided to the computer in its configuration.

remediate vulnerabilities and document those efforts in the remediation effort entry form.[33] NIST assigns severity levels to vulnerabilities by using the common vulnerability scoring system, a framework for communicating the characteristics of software vulnerabilities.[34] The scoring system captures the principal characteristics of a vulnerability and produces a numerical score reflecting its severity. Numerical scores are classified as risk levels (e.g., low, medium, high, or critical) to help organizations properly assess and prioritize vulnerability management processes. For example, on a scale of zero to 10, critical-risk vulnerabilities have a score from 9.0 to 10, while high-risk vulnerabilities have a score from 7.0 to 8.9. VA requires critical-risk vulnerabilities be remediated within 30 days and high-risk vulnerabilities be remediated within 60 days.

The inspection team reviewed 13 months of VA vulnerability scans, from November 2021 through November 2022. Based on these scan results, there were

- 444 high vulnerabilities on about 36 percent of computers that were remediated after the 60-day deadline,
- 405 critical vulnerabilities on about 15 percent of computers that were remediated after the 30-day deadline,
- 218 high vulnerabilities on about 35 percent of computers that were not remediated and were past the 60-day deadline for remediation, and
- 134 critical vulnerabilities on about 20 percent of computers that were not remediated and were past the 30-day deadline for remediation.

Without an effective patch management program, vulnerabilities such as security and functionality problems in software and firmware might not be mitigated, increasing opportunities for exploitation.

Finding 1 Conclusion

The OIT's vulnerability management reports in ICAMP were incomplete and inaccurate. Further, system vulnerabilities were not always remediated by deadlines established by VA. Without effective configuration management processes, users do not have adequate assurance

[33] A system 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. OIT Area Beckley, "Configuration Management."

[34] "Vulnerability Metrics," NIST National Vulnerability Database, accessed July 5, 2022, https://nvd.nist.gov/vuln-metrics/cvss; "Common Vulnerability Scoring System ver. 3.14, Specification Document, Revision 1," Forum of Incident Response and Security Teams (FIRST), accessed July 5, 2022, https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf.

that the system and network will perform as intended and to the extent needed to support VA missions.

Recommendations 1–2

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

1. Implement a process to minimize the Information Central Analytics and Metrics Platform data reliability issues.
2. Improve vulnerability management processes to ensure system changes occur within organization timelines.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendation 1 but did not concur with recommendation 2.

In addressing recommendation 1, the assistant secretary reported that VA made a correction to reflect a single name per computer for use during remediation and follow-up actions. Regarding recommendation 2, the assistant secretary said VA could provide evidence that it remedied the vulnerabilities that persisted beyond established remediation deadlines. The assistant secretary also stated that VA detects and addresses vulnerabilities persisting beyond identified remediation time frames and that are above configuration baselines as part of its standard patch and configuration management program, which includes timelines for testing, packaging, and phased deployment.

OIG Response

The assistant secretary for information and technology and chief information officer submitted a responsive action plan for recommendation 1. Further, the assistant secretary provided evidence to support actions addressing recommendation 1 were completed, and the OIG considers recommendation 1 closed.

Regarding recommendation 2, VA did not provide evidence that remediation efforts at the VA Beckley Healthcare System were successful. VA has implemented a newly established process to address vulnerability remediation at the system. In July 2023, OIT provided a document stating that plans of action and milestones were created for vulnerabilities that could not be remediated within established timelines on 0.54 percent of computers. However, this documentation is the result of processes established after the inspection team reported the remediation deficiency to VA. While this is a first step in addressing the report's findings with respect to vulnerability remediation, it does not demonstrate that the new process is working as intended. The OIG will continue to monitor the remediation of vulnerabilities and the creation of plans of action and

milestones for vulnerabilities that cannot be remediated during the information security inspections. Recommendation 2 will be closed when VA can demonstrate that the plan of action and milestone process can effectively mitigate security risks for unremedied security vulnerabilities. The full text of the assistant secretary's response is included in appendix D.

II. Security Management Controls

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.[35]

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

To assess security management controls, the inspection team reviewed local security management policies and standard operating procedures, as well as 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 topics reviewed were assessing and validating risks, 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.

Authorization to Operate

According to guidance, OIT issues an authorization to operate an information system and explicitly accepts the risk to agency operations, assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security and privacy controls.[36] The OIG determined that the VA Beckley Healthcare System's special-purpose IT system did not have an authorization to operate because it had not cleared the NIST risk management framework.[37] The special-purpose system included subsystems that monitor the distribution of oxygen throughout the hospital, alert facility police of emergencies via panic buttons, access the control room, and control the facility's climate.

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

[35] The security categorization indicates the minimum baseline controls needed to secure the system. *FISCAM* critical elements for security management are listed in appendix B.

[36] NIST Special Publication 800-53.

[37] 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.

acceptable level. A compromise of the special-purpose system's security could threaten the safety of patients, staff members, and visitors.

Security Categorization

When examining the special-purpose system at Beckley, the OIG found OIT did not consider all information types while establishing security category levels for similar systems at 137 VHA facilities. NIST's risk management framework requires the baseline controls for information systems be set based on the needs for confidentiality, integrity, and availability of the information within each system. Minimum security category settings—low, medium, or high—are used when determining baseline controls.

For example, the inspection team determined that 106 of the 137 VHA special-purpose systems included a network panic button system, which falls under the "emergency-response information" type that NIST recommends should have a security categorization of low for confidentiality, high for integrity, and high for availability. However, since OIT used a single standard for all special-purpose systems, 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. The "emergency response" information type was excluded because key facility personnel were not included in the security categorization process. While NIST allows the security categorization to be adjusted, OIT would need to document the rationale or justification for the adjustment. Documentation for that adjustment was not provided.

By not considering all information types during the security categorization, VHA healthcare system leaders do not have assurance that appropriate security and privacy controls were selected for special-purpose systems at their facilities to reduce the risk of compromise to an acceptable level.

Continuous Monitoring

During the inspection, the OIG discovered that plans of action and milestones were not created for 18 controls listed as noncompliant or unassessed in VA's Enterprise Mission Assurance Support Service. For instance, VA's Enterprise Mission Assurance Support Service indicated that the controls related to defining the personnel who can control the configuration of system logging functionality, and controls related to review, approval, implementation, and review of configuration changes were not assessed for compliance.[38] A plan of action and milestones would provide directions to implement and assess controls identified in VA's Enterprise Mission

[38] NIST Special Publication 800-53, AU-9(4) Access by Subset of Privileged Users and CM-3 Configuration Change Control.

Assurance Support Service as being noncompliant or not assessed. Without a plan of action and milestones, the risk presented by the vulnerability cannot be managed and resources needed for remediation may not be available.

Finding 2 Conclusion

The VA Beckley Healthcare System'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 facilities, and instead created a single security category for all special-purpose systems that did not have an authorization to operate. Additionally, plans of action and milestones had not been created for Beckley's IT security controls that were listed as noncompliant or unassessed in VA's Enterprise Mission Assurance Support Service. Without effective security management processes, users do not have adequate assurance that their IT systems and networks will perform as intended and to the extent needed to support VA missions.

Recommendations 3–5

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

3. Develop and approve an authorization to operate for the special-purpose systems.
4. 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.
5. Implement improved mechanisms to ensure system stewards are creating plans of action and milestones for all controls that have not been implemented or assessed.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 3 through 5. The assistant secretary reported that the work was completed and requested closure for recommendation 5.

In addressing recommendation 3, the assistant secretary reported that VA will develop and approve authorization packages for all special-purpose systems included in the system boundaries identified by the OIG. For recommendation 4, the assistant secretary stated that OIT is collaborating with VHA, Veterans Benefits Administration, and National Cemetery Administration business and information system owners to apply VA's approved assessment and authorization process for special-purpose systems in alignment with the NIST risk management framework. Further, the assistant secretary indicated that a VA authorizing official will assess the special-purpose system security plans and boundaries for an authority to operate. To address recommendation 5, the assistant secretary indicated facility staff addressed all unassessed

controls, added test results and evidence, and marked the controls as compliant on March 7, 2023.

OIG Response

The corrective action plans are responsive to the intent of the recommendations. OIT representatives indicated they are in the process of consolidating all special-purpose systems into a VA-wide authorization to operate. The OIG considers the planned September 2025 completion date to be reasonable for the actions planned in response to recommendations 3 and 4. The assistant secretary provided evidence to support actions addressing recommendation 5 were completed, and the OIG considers this recommendation closed.

The OIG will monitor implementation of the planned actions and will close recommendations 3 and 4 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.[39] Access also includes physical and environmental controls associated with physical security, such as authorization, visitors, monitoring, delivery, and removal. Identification, authentication, and authorization controls ensure that users have the proper access and access is restricted to authorized individuals. The inspection team reviewed five critical access control elements at the Beckley VA Medical Center, some of which contain multiple controls.[40]

Finding 3: The Beckley VA Medical Center Had Deficiencies in Five Access Controls

To evaluate the Beckley VA Medical Center's access controls, the inspection team interviewed the area manager, information system security officer, biomedical supervisor, database administrators, and local IT specialists. The team also reviewed local policies and procedures, conducted walk-throughs of the facility, and analyzed audit logs.[41]

The OIG found these issues with access controls at the Beckley VA Medical Center:

- Network segmentation controls to isolate several medical devices and special-purpose systems were not adequate or were missing.
- Uninterruptible power supplies to support equipment were lacking.
- The server room and several rooms containing infrastructure network equipment lacked physical controls.
- Several rooms containing infrastructure network equipment lacked environmental controls.
- Media was not being sanitized prior to disposal or reuse.

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

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

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

Network Segmentation Controls

The VA Beckley Healthcare System did not have network segmentation controls in place for several network medical and special-purpose system segments. Network segmentation controls regulate where information can travel within a system and between systems.[42]

Network-connected medical devices and special-purpose systems are placed on isolated network segments for protection. Protection is provided through access control lists.[43] However, the OIG identified seven network segments containing 39 special-purpose system devices that did not have access control lists applied. Further, an additional network segment that contained 90 Veterans Health Information System Technology Architecture imaging devices had access control lists applied, but the access control lists did not restrict access from the entire VA network. Finally, the healthcare system's network contained 941 devices that did not fall within a defined network segment used to identify whether access control lists needed to be applied. Without network segmentation controls in place, any user can access these potentially vulnerable medical devices. After the inspection team reported this issue to OIT, OIT provided support and applied appropriate access control lists to the network segments containing the medical devices after the OIG's site visit.

Uninterrupted Power Controls

The OIG determined that during the monthly generator test, the Beckley VA Medical Center loses power for approximately eight seconds each time the facility switches to and from generator power. The inspection team observed a generator test and determined that not all systems were connected to an existing or functional uninterrupted power supply. Consequently, the OIG observed the following:

- The emergency room nurses' central monitoring system, while connected to a nonfunctioning universal power supply, was down for under one minute. However, when the system came back online, the team noted that patient monitors that were not connected to patients started incorrectly sending audio alarms falsely indicating that they were removed from patients.
- The emergency room X-ray machines went offline and sent audio alarms when the power returned. Emergency room staff needed to contact radiology staff to reset the machines.
- The main phone line for radiology was down for over four minutes.

[42] NIST Special Publication, 800-53.

[43] Access control lists isolate network segments by limiting the resources that can be accessed within network segments.

- The police security cameras were reset and needed to be refocused to provide the necessary views.

The facility sends out an email warning staff that all elevators and electrical equipment, such as lights and computers will experience a brief loss of power at the start and end of the test. Further, an email is sent instructing staff that "OIT requests that all computers be logged off before each of these time frames when we experience a brief loss of power." Single points of failure could cause harm to patient care and degrade access to IT resources. During an actual power outage, the facility effects will be more severe than those experienced during the generator test, as the facility personnel would not have taken known precautions. Facility personnel have reported that power lapses have caused at least one issue that affected lab operations and another issue where there was a delay in a patient transfer.

Physical Controls

The medical center's computer room and 19 communication closets did not meet VA physical security requirements. Specifically, the facility's data lines were

- not all labeled,
- not using cable trays for protection,
- intertwined with electrical lines, and
- not directly plugged into patch panels.

Further, managers did not provide support to ensure that the carpeted raised tiles in the computer room would prevent electrical shocks. Finally, the computer room did not have hot and cold aisles that help units pull in cool air to prevent overheating.

Physical access is the process used to restrict an individuals' ability to enter computer rooms and communication closets to protect computer resources from intentional or unintentional loss or impairment.[44] The OIG found that the Beckley VA Medical Center did not adequately restrict access to its 19 communication closets and noted the following deficiencies, with some closets having more than one deficiency:

- Eleven were not monitored by camera.
- Five did not have an open-door alarm.
- Three did not have a backup deadbolt.
- One did not have personal identity verification card access enabled.

[44] NIST Special Publication 800-53; VA Directive 6500.

Inadequate physical controls could adversely affect IT operations and patient care.

Environmental Controls

The medical center's computer room and 19 communication closets did not meet federal and VA environmental security requirements. The OIG was informed that the facility's computer room experienced frequent water leaks. The OIG also noted that 24 incidents and repairs of leaks have occurred in the computer room or the adjacent telecommunication room since 2001. Additionally, the OIG found algae growth that could be attributed to standing water on the roof, ceiling tiles that were water damaged, and discolored fire retardant where water leaked from pipes exiting the computer room ceiling to the roof. Facility personnel showed the team rolls of plastic in the computer room that could be used to help protect equipment in the event a leak was detected. However, if a leak were to occur when no one was in the computer room, no other controls were in place to prevent water damage to the computer equipment.

Further, the facility had several deficiencies in IT environmental controls that protect computer resources from harm. The OIG found the following deficiencies when reviewing the 19 communication closets, with some closets having more than one deficiency:

- None had a smoke detector.
- Eighteen did not contain electrical grounding for equipment.
- Thirteen did not have temperature- and humidity-monitoring controls.
- Seven did not have an uninterrupted power supply.
- Five did not have fire suppression systems.

Without these environmental safeguards, organizational assets could be damaged by electrical surges, water, or fire, resulting in financial loss or harm to veterans.

Media Sanitization

The medical center was not sanitizing unencrypted hard drives prior to shipping the hard drives out for destruction. According to an OIT employee and corroborated by evidence collected, the facility damaged the hard drives using a method that would not destroy the data. Specifically, the facility personnel damaged the hard drive physical interface, not realizing that the drive could still be repaired and allow access to data contained on the drives.

Media protection personnel did not understand that this would not meet VA's media sanitization requirements. Hard drives that are not sanitized can lead to improper access to sensitive veteran information stored on media.

Finding 3 Conclusion

The Beckley VA Medical Center did not have network segmentation controls for some medical devices and special-purpose systems to protect them from unauthorized access. Furthermore, improvements are needed for the deployment of uninterruptible power supplies, which protect equipment in the event of a power outage. Additionally, physical and environmental security measures need to be improved to prevent destruction or harm to devices. Finally, media needs to be sanitized prior to disposal or reuse. Unless facility leaders take corrective actions, they risk unauthorized access to critical network resources, inability to respond effectively to incidents, and loss of personally identifiable information that can result in financial loss or harm to veterans.

Recommendations 6–10

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

6. Ensure network segmentation controls are applied to all network segments with special-purpose systems.

The OIG made four recommendations to the Beckley VA Medical Center director:

7. Install uninterruptible power supplies to eliminate single points of electrical failure supporting the facility.
8. Ensure that hot and cold aisles in computer rooms, and electric and data cables are installed in accordance with VA standards.
9. Validate that appropriate physical and environmental security measures are implemented and functioning as intended.
10. Implement media sanitization methods in accordance with VA policy requirements.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 6 through 10. The assistant secretary reported that the work was completed and requested closure for recommendation 6.

To address recommendation 6, the assistant secretary provided evidence that the medical center's OIT staff implemented appropriate network segmentation to protect all network devices on March 10, 2023. For recommendation 7, the assistant secretary stated that the medical center will purchase and install uninterruptible power supply units at each specific computer in the areas identified by the OIG. To address recommendation 8, the assistant secretary indicated the

medical center would implement hot and cold aisles in the computer room as part of the Electronic Healthcare Records Modernization project.

Regarding recommendation 9, the assistant secretary stated that in FY 2023, VA funded and initiated procurement of a maintenance project that will ensure the appropriate physical and environmental security measures are implemented and functioning, as identified by the OIG. For recommendation 10, the assistant secretary indicated that Beckley VA Medical Center facility staff have requested the purchase of a device that can be used to implement an Information System Security Manager-approved sanitization method.

OIG Response

OIT's corrective action plans are responsive to the intent of the recommendations. The assistant secretary provided evidence to support actions addressing recommendation 6 were completed, and the OIG considers this recommendation closed.

The OIG will monitor implementation of the planned actions and will close recommendations 7 through 10 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 Beckley. The 26 recommendations are listed below:

1. Consistently implement an improved continuous monitoring program in accordance with the National Institute of Standards and Technology (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.
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's authoritative system of record 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 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.
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 systems and applications are adequately logged and monitored to facilitate an agency-wide awareness of information security events.
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

The Government Accountability Office (GAO) developed the Federal Information System Controls Audit Manual (FISCAM) to provide auditors and information system control specialists with a methodology for evaluating the confidentiality, integrity, and availability of information systems. FISCAM groups related controls into categories that have similar risks. To assist auditors in evaluating information systems, FISCAM maps control categories to 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** by naming and describing the 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.[45] 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 by establishing effective programs for patch management, virus protection, and

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

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 management, 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 are needed to recover and support them.
- **Backup procedures and environmental controls** help prevent and minimize damage and interruption. 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 that lead 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 doing follow-up monitoring to ensure actions are effective. Agencies develop plans of action 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.[46]

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.
- **Controls over sensitive system resources** are designed to ensure the confidentiality, integrity, and availability of system data, and include things such as passwords and keys during transmission and storage. Technologies used to control sensitive data include encryption and certificate management.

[46] GAO, *FISCAM.*

- **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 authorized users can do, it grants or restricts user, service, or device access to various resources based on the identity of the user, service, device.

Federal Information Security Modernization Act (FISMA) of 2014

The stated goals of FISMA follow:

- 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.[47]

FISMA also requires an annual independent assessment of each agency's information security

[47] FISMA.

program to determine its effectiveness. Inspectors general or independent external auditors must 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 Interagency Working Group created the NIST information security guidelines.

Appendix C: Scope and Methodology

Scope

The inspection team conducted its work from September 2022 through May 2023. The team evaluated configuration management, security management, and access controls of operational VA information technology (IT) assets and resources in accordance with the Federal Information Security Modernization Act of 2014 (FISMA), National Institute of Standards and Technology (NIST) security guidelines, and VA's IT security 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 VA Beckley 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 any policy violations and threats to security.

Internal Controls

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

The team used the Government Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM) as a template to plan 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 FISCAM appendix II 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 VA Beckley Healthcare System 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 VA Office of Inspector General (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 Office of Information and Technology (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 their 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: July 7, 2023

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

Subj: Office of Inspector General Draft Report: Inspection of Information Security at the Beckley Healthcare System in West Virginia, Project Number 2023-00089-AE-002 (VIEWS 10265331)

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

1. The Office of Information and Technology (OIT) is responding to the Office of Inspector General (OIG) draft report, *Inspection of Information Security at the VA Beckley Healthcare System in West Virginia* (Project Number 2023-00089-AE-002).

2. OIT is submitting written comments, supporting documentation and a target completion date for each recommendation.

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,
Inspection of Information Security at the VA Beckley Healthcare System in West Virginia,
Project Number 2023-00089-AE-002
(VIEWS 10265331)

Recommendation 1: Implement a process to minimize the Information Central Analytics and Metrics Platform data reliability issues.

Comments: Concur.

The Department of Veterans Affairs (VA) Office of Information and Technology (OIT) concurs. The report used by the Office of Inspector General (OIG) to identify vulnerability remediation and mitigation actions displayed machine hostnames that conflicted with the vulnerability scanning tool. After review and analysis, VA corrected the report in the system to reflect a single hostname for use for remediation and follow-up actions. If any assets appear without a hostname on the vulnerability report, those assets go through name resolution processes and additional operational efforts to ensure appropriate tracking for remediation. Wherever possible, VA tracks and remediates vulnerabilities within policy-defined time frames based on criticality and risk. If VA cannot complete remediation within the defined time frame, VA enters a Plan of Action and Milestones (POAM) item for risk awareness and continuous monitoring of the vulnerability.

Expected Completion Date: Completed.

VA OIT requests closure of Recommendation 1.

Recommendation 2: Improve vulnerability management processes to ensure system changes occur within organization timelines.

Comments: Non-Concur.

VA can provide evidence of remediation of vulnerabilities that persist beyond established remediation time frames. VA continues to mature its POAM process for inclusion of related mitigation, business need and roadmap details, per the VA Material Weakness Roadmap. VA additionally detects and remediates vulnerabilities that persist beyond identified remediation time frames and that are above configuration baseline as part of VA's standard patch and configuration management program, which includes timelines for testing, packaging and phased deployment.

Expected Completion Date: Completed.

VA OIT requests removal or closure of Recommendation 2.

Recommendation 3: Develop and approve an authorization to operate for the special-purpose system.

Comments: Concur.

VA will develop and approve authorization packages for all special purpose systems (SPS) included in the system boundaries identified by the auditors.

Expected Completion Date: September 30, 2025.

Recommendation 4: 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 OIT, in collaboration with the Veterans Health Administration, Veterans Benefits Administration and National Cemetery Administration business and information system owners, is applying VA's approved assessment and authorization process for SPS in alignment with the National Institute for Standards and Technology Risk Management Framework. A VA authorizing official will assess the SPS system security plans and boundaries for an authority to operate.

Expected Completion Date: September 30, 2025.

Recommendation 5: Implement improved mechanisms to ensure system stewards are creating plans of action and milestones for all controls that have not been implemented or assessed.

Comments: Concur.

Beckley VA Medical Center (VAMC) staff addressed all unassessed controls, added test results and evidence and marked the controls as compliant on March 7, 2023. VAMC staff additionally uploaded evidence to meet the criteria of each control and generated zero POAM items.

Expected Completion Date: Completed.

VA OIT requests closure of Recommendation 5.

Recommendation 6: Ensure network segmentation controls are applied to all network segments with special-purpose systems.

Comments: Concur.

Beckley VAMC OIT staff implemented appropriate network segmentation to protect all network devices on March 10, 2023. Beckley VAMC staff provided supporting evidence to satisfy the security requirements.

Expected Completion Date: Completed.

VA OIT requests closure of Recommendation 6.

Recommendation 7: Install uninterruptible power supplies to eliminate single points of electrical failure supporting the facility.

Comments: Concur.

Beckley VAMC will purchase and install uninterruptible power supply units at each specific computer in the areas identified by the auditors.

Expected Completion Date: September 30, 2023.

Recommendation 8: Ensure that hot and cold aisles in computer rooms, and electric and data cables are installed in accordance with VA standards.

Comments: Concur.

Beckley VAMC initiated the Electronic Healthcare Records Management (EHRM) project to address the identified issues. The planning stage of the project is 35% complete.

Expected Completion Date: September 30, 2026.

Recommendation 9: Validate that appropriate physical and environmental security measures are implemented and functioning as intended.

Comments: Concur.

Within the Fiscal Year 2023 Operating Plan, Veterans Integrated Service Network 5 funded a maintenance project, for which Beckley VAMC Facilities Management is currently preparing a contracting package for solicitation; this effort is expected to be completed by August 31, 2024. Beckley VAMC Facility Management Services staff expects to fully complete the maintenance project by February 29, 2024. The project will ensure the appropriate physical and environmental security measures are implemented and functioning, as identified by the OIG.

Expected Completion Date: August 31, 2024.

Recommendation 10: Implement media sanitization methods in accordance with VA policy requirements.

Comments: Concur.

Beckley VAMC facility staff have requested an Information System Security Manager-approved sanitization method. The facility staff requested a quote and entered a VA Form 2237 for approval. Once approved, the transaction item needs to be obligated, and funds acquired before the facility may purchase and receive the sanitization device.

Expected Completion Date: September 30, 2023.

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 Brandon Zahn
Other Contributors	Dustin Campbell Charles Hoskinson Melinda Peal Bishop 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

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
U.S. Senate: Joseph Manchin III, Shelley Moore Capito
U.S. House of Representatives: Carol Miller

OIG reports are available at www.va.gov/oig.