US DEPARTMENT OF VETERANS AFFAIRS

# OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

## VETERANS HEALTH ADMINISTRATION

# Follow-Up Inspection of Information Security at the VA Beckley Healthcare System in West Virginia


| Information Security Inspection | 24-03708-141 | January 29, 2026 |
|---|---|---|


## OUR MISSION

To conduct independent oversight of the Department of Veterans Affairs that combats fraud, waste, and abuse and improves the effectiveness and efficiency of programs and operations that provide for the health and welfare of veterans, their families, caregivers, and survivors.

## CONNECT WITH US

**Subscribe** to receive updates on reports, press releases, congressional testimony, and more. Follow us at @VetAffairsOIG.

## PRIVACY NOTICE

In addition to general privacy laws that govern release of medical information, disclosure of certain veteran health or other private information may be prohibited by various federal statutes including, but not limited to, 38 U.S.C. §§ 5701, 5705, and 7332, absent an exemption or other specified circumstances. As mandated by law, the OIG adheres to privacy and confidentiality laws and regulations protecting veteran health or other private information in this report.

# Executive Summary

The VA Office of Inspector General (OIG) conducted a follow-up inspection of the VA Beckley Healthcare System in West Virginia to assess compliance with federal cybersecurity standards under the Federal Information Security Modernization Act of 2014 (FISMA).[1] This healthcare system was previously inspected by the OIG in 2023 and was selected for follow-up to determine whether VA had taken appropriate corrective actions to address the OIG's 10 recommendations from the prior inspection.[2] This inspection focused on three security control categories: configuration management, security management, and access controls. The inspection team concluded that VA had made substantial progress in addressing the recommendations from the previous OIG report.

The OIG conducted a site visit to the VA Beckley Healthcare System in West Virginia during the week of October 21, 2024. The OIG made five recommendations to improve configuration management, security management, and access controls to safeguard veterans' information.[3] The acting assistant secretary for VA's Office of Information Technology (OIT) and chief information officer noted that VA concurred with recommendations 1, 2, 3, and 5. VA requested closure of recommendations 2, 3, and 5 and provided documentation of completed corrective actions. The OIG considers recommendations 2, 3, and 5 closed. However, VA did not concur with recommendation 4, which addressed access controls for a specific system. The acting assistant secretary said all activities in the system are tracked and reportable and said restricting access based on certain roles would present a challenge because all personnel in that service need access. VA provided evidence of the facility limiting the administrator key, as well as service administration team members and facility leaders recognizing and assuming the risk. Based on this, the OIG considers recommendation 4 closed as VA's actions meet the intent of the recommendation.

In December 2024, the OIG provided VA with details of its preliminary findings and recommendations. As reflected above, during 2025, VA worked to address the OIG's preliminary findings and recommendations, and VA filed a formal response to the OIG's recommendations in September 2025. The communication of preliminary findings and recommendations to VA contained "VA Sensitive Data" as defined in section 5727 under Title 38 of the United States Code (U.S.C.). Federal law, including FISMA and its implementing regulations, requires federal agencies to protect sensitive data and information systems due to the

[1] The scope and methodology of this follow-up inspection are detailed in appendix A.

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

[3] The full list of recommendations can be found in the report along with VA's response and action plan, which is available in appendix D.

risk of harm that could result from improper disclosure. Accordingly, that material is not being published by the OIG or distributed outside VA.

## What the Follow-Up Inspection Found

The OIG team identified continued deficiencies in all three control areas inspected: configuration management, security management, and access controls. For configuration management, the OIG concluded that the healthcare system did not meet required timelines for addressing critical vulnerabilities and lacked necessary remediation plans, leaving outdated software on numerous systems. Additionally, the OIG identified several unique high and critical vulnerabilities within the network that were not reflected in the agency's standard vulnerability reports.

The OIG found three major security management deficiencies in the healthcare system that put veterans' personal data at risk. The healthcare system lacked an authorization to operate a special-purpose system, which could compromise the system's security—potentially threatening patient safety and staff well-being. OIT did not document the consideration of the impact on human life when establishing the security category level for a national special-purpose system, which could result in incorrect risk levels. Lastly, the healthcare system did not ensure appropriate separation of duties for managing the inventory of noncontrolled substances in the related system, which could result in undetected diversion of items from that inventory.

The inspection team determined that the healthcare system made progress in improving access controls by restricting access to the computer room and 19 communications closets and by directly plugging data lines into patch panels; however, work was still in progress during the follow-up inspection. The deputy chief information officer for compliance, risk, and remediation reported the target completion date is September 30, 2026. However, the team found that a contractor's on-site destruction of temporary paper records that contained personally identifiable information was not observed by a witness, as required.[4] Without an observer, VA has no assurance these records were destroyed.

## Next Steps

The OIG will monitor implementation of the remaining planned actions and will close recommendation 1 when VA provides evidence demonstrating implemented processes to ensure

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

all vulnerabilities are identified and plans of action and milestones are created for vulnerabilities that cannot be mitigated by VA deadlines.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

# Contents

# Abbreviations

| | |
|---|---|
| FISCAM | Federal Information System Controls Audit Manual |
| FISMA | Federal Information Security Modernization Act of 2014 |
| FY | fiscal year |
| GAO | Government Accountability Office |
| IT | information technology |
| NIST | National Institute of Standards and Technology |
| OIG | Office of Inspector General |
| OIT | Office of Information and Technology |
| OMB | Office of Management and Budget |
| U.S.C. | United States Code |
| VHA | Veterans Health Administration |

# Introduction

Information security controls protect VA systems and data from unauthorized access, use, modification, and destruction. To determine compliance with the Federal Information Security Modernization Act of 2014 (FISMA), the VA Office of Inspector General (OIG) contracts with an independent public accounting firm that conducts an annual audit of VA's information security program and practices.[5] The FISMA audit is conducted in accordance with guidelines issued by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST).

In 2020, the OIG started an information security inspection program. These inspections provide recommendations to VA on enhancing information security oversight at local and regional facilities.[6] Typically, facilities selected for these inspections either were not included in the annual FISMA sample or had previously performed poorly.

The OIG previously inspected the VA Beckley Healthcare System in West Virginia in 2023 and made 10 recommendations to correct identified security weaknesses.[7] This follow-up inspection was conducted to determine whether the healthcare system's information security systems were meeting federal security guidance and whether VA has taken appropriate corrective actions.[8] The inspection team visited the Beckley VA Medical Center in West Virginia during the week of October 21, 2024. The team reviewed configuration management, continuity planning, security management, and access controls. The team found VA's Office of Information Technology (OIT) made substantial progress in addressing the recommendations from the 2023 OIG report.

In December 2024, the inspection team provided OIT with details of its preliminary findings and recommendations. During 2025, VA worked to address the OIG's preliminary findings and recommendations, and VA filed a formal response to the OIG's recommendations in September 2025. The communication of preliminary findings and recommendations to VA contained "VA Sensitive Data" as defined in section 5727 under Title 38 of the United States Code (U.S.C.). 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

[5] Federal Information Security Modernization Act (FISMA) of 2014, 44 United States Code (U.S.C.) §§ 3551–3558; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2024*, Report No. 24-01233-90, June 18, 2025.

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

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

[8] Appendix A provides more detail on this inspection's scope and methodology, appendix B details the fiscal year (FY) 2024 FISMA audit recommendations, and appendix C presents information about FISMA and other federal criteria and standards discussed in this report.

result from improper disclosure. Accordingly, that internal material is not being published by the OIG or distributed outside VA.

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

## Security Controls

Both OMB and NIST provide criteria for implementing security controls.[9] These criteria call for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system.

VA guidance outlines both NIST- and VA-specific requirements to help information system owners select the appropriate controls to secure their systems.[10] NIST defines a system owner as a "person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system."[11] According to VA Directive 6500, responsibility for developing and maintaining information security policies, procedures, and control techniques lies with the assistant secretary for information and technology, who also serves as VA's chief information officer. VA Handbook 6500 describes the risk-based process for selecting system security controls, including operational requirements.

This OIG information security inspection focused on three security control areas selected based on their level of risk, as shown in table 1. Weaknesses in these controls can result in unauthorized access to, modification of, or disclosure of VA sensitive data and programs and disruption of critical operations.[12]

**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 |

[9] OMB, "Security of Federal Automated Information Resources," app. III in OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016; NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, September 23, 2020.

[10] VA Handbook 6500, *Risk Management Framework for VA Information Systems: VA Information Security Program*, February 2021; VA Directive 6500, *VA Cybersecurity Program*, February 24, 2021.

[11] NIST Computer Security Resource Center, Glossary, "system owner," accessed February 22, 2025, https://csrc.nist.gov/glossary/term/system_owner.

[12] Government Accountability Office (GAO), *Federal Information System Controls Audit Manual (FISCAM)*, GAO-24-107026, September 2024.

| Control area | Purpose | Examples evaluated |
|---|---|---|
| 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 of FISCAM.*

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

## OIT Structure and Responsibilities

The assistant secretary for information and technology leads OIT. Figure 1 on the next page shows the OIT offices relevant to the areas the OIG team assessed at the VA Beckley Healthcare System.

OIT's End User Operations team provides on-site support to information technology (IT) customers across all VA administrations and program offices—including VA employees and contractors with government-furnished IT equipment and access. End User Operations staff assigned to the VA Beckley Healthcare System are responsible for managing system plans of action and milestones to ensure all assessed and scanned vulnerabilities are documented.[13]

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

[13] VA OIT, End User Services (EUS), *End User Operations (EUO), Security Controls - Risk Assessment (RA) Standard Operating Procedure (SOP)*, ver. 1.0.3, March 18, 2025.

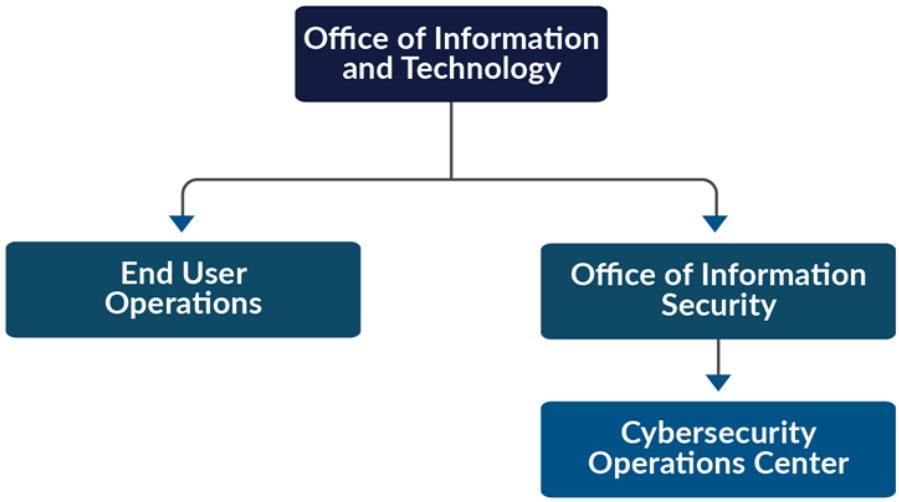


***Figure 1.*** *Organizational structure of OIT entities relevant to this inspection.*
*Source: VA OIG analysis of the VA Functional Organization Manual, version 8, dated 2023.*

## Results of Previous Projects

The OIG's fiscal year (FY) 2024 FISMA audit evaluated 49 major applications and general support systems hosted at 23 VA facilities and tested selected security and privacy controls outlined by NIST.[14] The audit report included 23 recommendations, which are listed in appendix B. Of the 23 recommendations, 21 were repeated from the prior annual audit, indicating VA continues to face significant challenges in complying with FISMA requirements.[15] Repeat recommendations included addressing deficiencies in configuration management, security management, and access controls.

The Government Accountability Office (GAO) has also found that VA has a deficient information security program. GAO reported in 2023 that VA faced several security challenges while securing and modernizing its information systems, including

- fully implementing a process for privacy officials to review IT capital investment plans and budget requests;
- establishing clear privacy workforce management procedures, involving the senior agency officials for privacy in hiring, training, and professional development to identify staffing requirements and ensure a qualified workforce;

[14] According to the NIST Computer Security Resource Center Glossary, a general support system is an interconnected set of information resources under the same direct management control that share common functionality. "Glossary" (web page), NIST Computer Security Resource Center, accessed September 3, 2025, https://csrc.nist.gov/glossary/term/general_support_system.

[15] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2024*. See appendix B for more information.

- fully defining and documenting the role of privacy officials in authorizing information systems with personally identifiable information, as their involvement is not always documented in policies and procedures;
- fully developing a continuous monitoring strategy; and
- providing continual attention to key elements in its cybersecurity risk management strategy, an agencywide risk assessment, and identification of enterprise cybersecurity risks, and coordinating between its cybersecurity risk executive and enterprise risk management functions.[16]

As mentioned, the OIG previously inspected the VA Beckley Healthcare System in 2023 and made 10 recommendations to correct identified security weaknesses.[17]

## VA Beckley Healthcare System

The VA Beckley Healthcare System consists of the Beckley VA Medical Center (shown in figure 2), the Princeton and Greenbrier community-based outpatient clinics, and a VA mobile clinic. In FY 2024, the medical center provided care to over 13,000 patients, had 964 employees, and a budget of over $248 million, according to OIT documents.


***Figure 2.*** *Beckley VA Medical Center in West Virginia.*
*Source: https://www.va.gov/beckley-health-care/ (accessed September 11, 2024).*

[16] GAO, *Cybersecurity: VA Needs to Address Privacy and Security Challenges*, GAO-23-106412, April 18, 2023.
[17] VA OIG, *Information Security Inspection at the VA Beckley Healthcare System in West Virginia.*

# Results and Recommendations

The inspection team reviewed configuration management, security management, and access controls at the VA Beckley Healthcare System—areas determined to be of the highest risk for not adequately protecting veterans' sensitive data based on the OIG's previous report. Although the healthcare system had improved since the previous inspection, the team identified persistent deficiencies related to configuration management, security management controls, and access controls. Table 2 summarizes the findings and recommendations from the prior inspection and shows whether facility managers implemented effective controls to address prior recommendations or whether the problems persisted, resulting in repeat findings in FY 2025.

**Table 2. Evaluation of Actions Addressing Prior Recommendations for the VA Beckley Healthcare System**

| Control area | Prior finding | Prior recommendation | Repeat finding in FY 2025 |
|---|---|---|---|
| Configuration management | VA's vulnerability reports for the healthcare system contained inaccurate and incomplete information. | Implement a process to minimize the Information Central Analytics and Metrics Platform data reliability issues. | No |
| Configuration management | The healthcare system did not identify and remediate all critical or high vulnerabilities in the network. | Improve vulnerability management processes to ensure system changes occur within organization timelines. | Yes |
| Security management | The healthcare system's special-purpose IT system did not have an authorization to operate because it had not cleared the NIST risk management framework. | Develop and approve an authorization to operate for the special-purpose systems. | Yes |
| Security management | OIT did not consider all information types while establishing security category levels for special-purpose systems at Beckley and 137 healthcare systems. | 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. | Yes |
| Security management | Plans of action and milestones were not created for 18 controls listed as noncompliant or unassessed in VA's Enterprise Mission Assurance Support Service. | Implement improved mechanisms to ensure system stewards are creating plans of action and milestones for all controls that have not been implemented or assessed. | No |

| Control area | Prior finding | Prior recommendation | Repeat finding in FY 2025 |
|---|---|---|---|
| Access | Network segmentation controls to isolate several medical devices and special-purpose systems were not adequate or were missing. | Ensure network segmentation controls are applied to all network segments with special-purpose systems. | No |
| Access | Uninterruptible power supplies to support equipment were lacking. | Install uninterruptible power supplies to eliminate single points of electrical failure supporting the facility. | No |
| Access | The server room and several rooms containing infrastructure network equipment lacked physical controls. | Ensure hot and cold aisles in computer rooms and electric and data cables are installed in accordance with VA standards. | Yes |
| Access | Several rooms containing infrastructure network equipment lacked environmental controls. | Validate that appropriate physical and environmental security measures are implemented and functioning as intended. | No |
| Access | Media were not sanitized before disposal or reuse. | Implement media sanitization methods in accordance with VA policy requirements. | No |

*Source: VA OIG analysis of follow-up inspection results and prior report findings (VA OIG,* Information Security Inspection at the VA Beckley Healthcare System in West Virginia*, Report No 23-00089-144, September 21, 2023).*

While the VA Beckley Healthcare System improved its configuration management processes to address some deficiencies, the OIG team identified repeat security weaknesses related to vulnerability remediation processes designed to protect sensitive information.

During the review of security management controls, the team identified deficiencies in user account management, system authorization and assigning a security categorization for special-purpose systems, and segregating pharmaceutical system administrator duties from individuals with access to noncontrolled substances.

Finally, the team identified persistent deficiencies in physical access controls. In short, although the healthcare system made progress, the OIG will continue to track efforts toward completing these prior recommendations.

## I. Configuration Management Controls

According to GAO's *Federal Information System Controls Audit Manual* (*FISCAM*), configuration management involves identifying and managing security features for all hardware, software, and firmware components of an information system at a given point and systematically

controlling changes to that configuration during the system's operation.[18] An effective configuration management process should be described in a configuration management plan and then implemented according to that plan. OIT's Cybersecurity Operations Center identifies and reports on threats and vulnerabilities within VA. Vulnerabilities that cannot be remediated by OIT at the enterprise level are referred to OIT staff assigned to specific facilities. This helps secure devices from attack. The OIG inspection team examined whether the VA Beckley Healthcare System identified and remediated vulnerabilities within established time frames and configured its servers according to standards.

## Finding 1: The Healthcare System Had One Deficiency in Configuration Management

The team concluded that the healthcare system had a deficiency in configuration management controls over vulnerability remediation. A vulnerability is a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source."[19]

### Vulnerability Management

FISMA audits have repeatedly found deficiencies in VA's vulnerability management controls. Consistent with those findings, the team identified deficient controls at the VA Beckley Healthcare System. This is a repeat finding from the previous site inspection.

Vulnerability management is how an organization identifies, classifies, and reduces weaknesses, and it helps the organization assess risks and monitor the effectiveness of its overall security program. At VA, OIT conducts both routine and random vulnerability scans and reports the identified vulnerabilities to facilities for remediation. In calendar year 2023, OIT implemented a formal process to track the monitoring and remediation of vulnerabilities nationwide by using a plan of action and milestones. However, as of this follow-up inspection, the new process was not in place long enough to demonstrate effectiveness at remediating security vulnerabilities. The OIG also notes that the repeat vulnerability management finding was initially communicated to OIT in September 2023, and the resulting remediation plan had not been fully implemented over a year later.

The new tracking process makes information system stewards responsible for entering all critical and high-severity vulnerabilities that cannot be remediated on time (within 60 days) into a plan

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

[19] GAO, *FISCAM*.

of action and milestones for mitigation. Information system stewards should then use a prescribed form to provide evidence showing that the deficiencies have been mitigated.[20]

NIST guidance calls for a severity level to be assigned to each vulnerability using the Common Vulnerability Scoring System.[21] The inspection team's testing of vulnerability remediation focused on whether critical and high-severity vulnerabilities were remediated within agency-approved timelines, as shown in table 3.

**Table 3. Vulnerability Remediation Timelines by Severity Level**

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

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

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

The inspection team compared the results of the OIT-provided network vulnerability scan from the VA Beckley Healthcare System against OIG scans conducted from October 21 through October 24, 2024. OIT and the inspection team used the same vulnerability scanning tools. The OIG identified a critical vulnerability and several high-severity vulnerabilities on multiple hosts that were not identified in the agency's vulnerability reports. According to NIST, "A host is any hardware device that has the capability of permitting access to a network via a user interface, specialized software, network address, protocol stack, or any other means."[22] Both the OIG and OIT scans showed a high number of vulnerabilities persisting past deadlines.

The inspection team found the VA Beckley Healthcare System continued to experience a number of unresolved security vulnerabilities that exceeded established remediation timelines. These included both critical and high-severity issues affecting multiple systems and hosts, some of which had been present on the network for several months without documented remediation plans.

[20] An information system steward is an agency official with legal or operational authority for specified information who is responsible for establishing controls for its generation, collection, processing, dissemination, and disposal. NIST Computer Security Resource Center, *Glossary*, "information steward," accessed November 13, 2024, https://csrc.nist.gov/glossary/term/information_steward.

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

[22] NIST Computer Security Resource Center, "host," accessed February 13, 2025, https://csrc.nist.gov/glossary/term/host.

The inspection team found the vulnerabilities identified as exploitable by federal cybersecurity guidance generally had remediation plans when they remained unresolved beyond 60 days. However, some of these vulnerabilities were not fully addressed within recommended remediation timelines, including several classified as high and critical severity across multiple systems.[23]

### Finding 1 Conclusion

Numerous system vulnerabilities were not mitigated within established time frames. These vulnerabilities created security weaknesses on the VA Beckley Healthcare System's network that could be exploited to gain unauthorized access or disrupt operations.

## Recommendation 1

The OIG made the following recommendation to the assistant secretary of information and technology, who also serves as the chief information officer:[24]

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

## VA Management Comments

The acting assistant secretary for information and technology concurred with recommendation 1, stating that the Beckley medical facility is working with system stakeholders to ensure plans of action and milestones are created for vulnerabilities that cannot be mitigated in accordance with VA timelines. The full text of the acting assistant secretary's response is included in appendix D.

## OIG Response

The planned corrective actions are responsive to the intent of the recommendation. The OIG will monitor implementation of the planned action and will close recommendation 1 when VA provides evidence demonstrating progress in addressing the identified issues.

[23] "Known Exploited Vulnerabilities Catalog" (web page), Cybersecurity & Infrastructure Security Agency, accessed November 7, 2024, https://www.cisa.gov/known-exploited-vulnerabilities-catalog. This catalog provides due dates for remediation actions of each known exploited vulnerability.

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

## II. Security Management

According to *FISCAM*, "the security management program should establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures."[25] The inspection team evaluated three critical elements of security management: authorization to operate, security categorization, and continuous monitoring.[26] The security categorization indicates the minimum baseline controls needed to secure the system.

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

## Finding 2: The Healthcare System Had Three Deficiencies in Security Management

The inspection team identified deficiencies with authorizations to operate, security categorization, and separation of duties.

### Authorization to Operate

OIT issues an authorization to operate for each information system and, based on that formal document, 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.[27] The OIG team found the VA Beckley Healthcare System's special-purpose IT system did not have an authorization to operate. The area manager did not implement one because VA is developing an authorization to operate for all special-purpose systems at the enterprise level, which has not yet cleared the NIST risk management framework.[28] This is a

[25] GAO, *FISCAM*.

[26] *FISCAM* critical elements for security management are listed in appendix C.

[27] NIST Special Publication 800-53.

[28] VA's Enterprise Mission Assurance Support Service states that the special-purpose system comprises "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," accessed February 27, 2025, https://va.emass.apps.mil/App/CA/SystemDetails/2561/8541. (This website is not publicly accessible.) The NIST risk management framework integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle. Managing organizational risk is paramount to effective information security and privacy programs.

repeat finding from the OIG's previous site visit. The special-purpose system included systems that monitor the distribution of oxygen throughout the hospital, alert facility police of emergencies, 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 acceptable level. A compromise of the special-purpose system's security could threaten the safety of patients, staff members, and visitors.

## Security Categorization

During the prior inspection, the OIG team determined OIT did not consider all information types while establishing security category levels for special-purpose systems for 137 healthcare systems in the Veterans Health Administration (VHA). When examining the special-purpose system at Beckley, the OIG learned that OIT plans to create a national special-purpose system for 137 facilities. However, the OIG determined that OIT did not document the consideration of the impact of special-purpose systems to human life for these facilities.

For example, the inspection team determined that 117 of the 137 healthcare systems included a network system, which falls under "emergency response" information. NIST recommends that this type of information system should have a security categorization of "low" for confidentiality, "high" for integrity, and "high" for availability. Specifically, according to NIST standards, these 117 systems should have a categorization of "high" for confidentiality and availability if the loss of either could "result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries."[29]

When determining the baseline security categorization, OIT used three information types for all special-purpose systems: "personal identity and authentication information," "general information," and "system and network monitoring." However, the "emergency response" information type was excluded, and OIT assigned the enterprise special-purpose system a security risk categorization of "moderate" for confidentiality, integrity, and availability. This risk rating is suitable for the three security categorizations identified but is not suitable for emergency response systems due to their potential impact to human life. Although NIST allows the security categorization to be adjusted, OIT would need to document the rationale or justification for such an adjustment and had not done so.

Because OIT did not consider the impact to human life 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.

[29] NIST, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards Publication (FIPS Pub), February 2004.

### Separation of Duties

The VA Beckley Medical Center pharmacy uses a specific application to manage the inventory of noncontrolled substances.[30] Six pharmacy employees had access to noncontrolled substances *and* can administer the application user accounts.[31] Having both access to noncontrolled substances and administrative access in the application creates an opportunity to bypass inventory controls. Federal and VA requirements state that incompatible duties should be performed by separate individuals.[32] This means system administration should not be performed by an individual who has custody of noncontrolled substances. The lack of separation of duties creates a situation that could allow undetected diversion of that inventory.

### Finding 2 Conclusion

The VA Beckley Healthcare System's special-purpose IT system did not have an authorization to operate. Furthermore, OIT did not consider all information types when performing risk assessments of similar systems across 137 VA facilities and created a single security category for all special-purpose systems that did not have an authorization to operate. 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's mission.

## Recommendations 2–4

The OIG made the following recommendations to the assistant secretary of information and technology, who also serves as the chief information officer:[33]

2. Develop and approve an authorization to operate for the special-purpose systems.

[30] The inventory of noncontrolled substances within the application includes antibiotics, clomiphene citrate, and sildenafil. The inventory of controlled substances and antihistamines is maintained in the Veterans Health Information Systems and Technology Architecture.

[31] Administrative access allows the chief of pharmacy, associate chief of pharmacy, pharmacy operations supervisor, pharmacy informatics program manager, community care pharmacy program manager, and procurement pharmacy program manager to add and remove user accounts, change passwords belonging to accounts, and assign privileges to accounts within the application.

[32] NIST Special Publication 800-53; "Security Controls Explorer" (web page), VA Information Security Knowledge Service, accessed December 30, 2024, https://dvagov.sharepoint.com/sites/OITOIS/KnowledgeService/Pages/SecurityControls.aspx (This website is not publicly accessible.); VHA Directive 1108.07(1), *Transmittal Sheet General Pharmacy Service Requirements*, November 28, 2022.

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

3. Include facility personnel during the security categorization process to ensure all necessary information types are considered when determining the security categorization for special-purpose systems.

The OIG made the following recommendation to the Beckley VA Medical Center director:[34]

4. Segregate the pharmacy application administrative access from individuals who are custodians of the pharmaceutical inventory.

## VA Management Comments

The acting assistant secretary for information technology concurred with recommendations 2 and 3. For recommendation 2, the acting assistant secretary reported that the Special Purpose-Legacy Information Technology Environment received an authorization to operate in February 2025. For recommendation 3, he said system personnel were included in the security categorization process before granting the authorization to operate in April 2025.

The acting assistant secretary did not concur with recommendation 4. He said that implementing separation of duties for administrator access in the pharmacy application is challenging and inefficient, as all pharmacy staff need access to medications. Additionally, the assistant secretary said pharmacy technicians handle inventory updates to aid procurement activities and all actions in the application are tracked and reportable. The full text of the acting assistant secretary's response is included in appendix D.

## OIG Response

For recommendations 2 and 3, the corrective actions are responsive to the intent of the recommendation. Based on the actions taken and evidence provided by VA, the OIG considers recommendations 2 and 3 closed.

For recommendation 4, although VA did not concur with the recommendation to restrict access, VA's actions to limit personnel access are acceptable. VA provided evidence of the facility limiting the pharmacy administrator key and of pharmacy administration team members and facility leaders recognizing and assuming the risk. Based on this, the OIG considers recommendation 4 closed as VA's actions meet the intent of the recommendation.

[34] The recommendations addressed to the medical center director are directed to anyone in an acting status or performing the delegable duties of the position.

## III. Access Controls

Previous FISMA reports have repeatedly identified access controls as a nationwide issue for VA. Access controls—including boundary protections, sensitive system resources, physical security, and audit and monitoring controls—provide reasonable assurance that computer resources are restricted to authorized individuals.[35] Access controls can be logical or physical:

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

Identification, authentication, and authorization controls ensure users have proper access and that access is restricted to authorized individuals. At the VA Beckley Healthcare System, the inspection team reviewed access and environmental controls over the computer room and communications closets.[36]

To assess security management controls, the inspection team reviewed local security management policies, standard operating procedures, and applicable VA policies. These included documentation from the Enterprise Mission Assurance Support Service. The team interviewed the information system security manager, information system security officers, biomedical staff, and the area manager. The team also conducted a walk-through of the Beckley VA Medical Center. Security management controls reviewed included user management and oversight of medical devices.

### Finding 3: The Healthcare System Had Deficiencies with Two Access Controls

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

#### Physical Controls

The inspection team determined that the medical center made progress by addressing the OIG's previous recommendations. While corrective actions were made like directly plugging data lines into patch panels, some deficiencies—including the need for hot and cold aisles—were ongoing. The deputy chief information officer for compliance, risk, and remediation reported the targeted completion date to correct those issues is September 30, 2026.

[35] GAO, *FISCAM*.

[36] *FISCAM* critical elements for access controls are listed in appendix C.

### Monitoring Destruction of Temporary Records

The healthcare system did not have a witness observe a contractor's on-site destruction of temporary paper records that contained personally identifiable information.[37] Federal and VA requirements say a witness must observe the destruction of such documents; however, no witness observed the destruction of these documents at the medical center.[38] Facility security footage showed a contractor loaded the documentation into a truck at the medical center, where the contractor stated the documentation was destroyed; however, the security cameras could not capture anything that happened inside the truck. As a result, the healthcare system has no assurance the paper records were destroyed. A compromise of these temporary paper records could result in financial and reputational loss to VA, which is entrusted to protect sensitive veteran data.

### Finding 3 Conclusion

The VA Beckley Healthcare System made significant progress in correcting physical controls. For the remaining physical control issues, the targeted completion is September 30, 2026. Regarding controls over physical records, the healthcare system did not ensure a witness observed a contractor destroying sensitive paper records, which risks unauthorized access, disruption, and destruction of critical resources.

## Recommendation 5

The OIG made the following recommendation to the Beckley VA Medical Center director:[39]

5. Ensure a witness observes the destruction of temporary paper files that contain personally identifiable information and protected health information.

## VA Management Comments

The acting assistant secretary for information technology concurred with recommendation 5. He noted that the VA Beckley Medical Center designated an employee in the Privacy Office to witness the destruction of paper files sent to the shredding vehicle and that the Privacy Office will verify the destruction through documentation certifying that the established process was

[37] According to VA Directive 6371, *Destruction of Temporary Paper Records*, April 8, 2014, the "destruction carried out by an information destruction contractor must be witnessed by a VA employee or, if authorized by the VA organization that created the temporary paper records, a contractor (or subcontractor or third party) employee may act as witness."

[38] 36 C.F.R. § 1226.24; "Disposition of Federal Records: A Records Management Handbook" (web page), National Archives Administration, accessed November 18, 2024, https://www.archives.gov/files/records-mgmt/pdf/dfr-2000.pdf; VA Directive 6371.

[39] The recommendations addressed to the medical center director are directed to anyone in an acting status or performing the delegable duties of the position.

followed. He stated that the corrective action was completed in April 2025 and requested closure. The full text of the acting assistant secretary's response is included in appendix D.

## OIG Response

The corrective actions are responsive to the intent of recommendation 5. Based on the actions taken and evidence provided by VA, the OIG considers recommendation 5 closed.

# Appendix A: Scope and Methodology

## Scope

The VA Office of Inspector General (OIG) inspection team conducted its work from September 2024 through April 2025. The team evaluated configuration management, security management, and access controls of operational VA information security assets and resources in accordance with the Federal Information Security Modernization Act (FISMA), National Institute of Standards and Technology (NIST) security guidelines, and VA's information security policy. In addition, the team assessed the capabilities and effectiveness of information security controls used to protect VA systems and data from unauthorized access, use, modification, or destruction.

## Methodology

To accomplish the objective, the inspection team examined relevant laws and policies and inspected the VA Beckley Healthcare System and its information systems for security compliance. Additionally, the team interviewed VA staff responsible for the facility's information technology security and operations. Furthermore, the team conducted an on-site physical security review of the VA Beckley Medical Center. To determine local systems' security compliance, the team conducted vulnerability and configuration testing for the VA Beckley Healthcare System at the VA Beckley Medical Center. Finally, the team analyzed the results of testing, interviews, and the inspection to identify policy violations and threats to security.

## Internal Controls

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

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

However, some controls overlap and are included in both assessments due to redundant roles and responsibilities among VA's local, regional, and national facilities and offices.

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

## Data Reliability

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

## 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 B: Recommendations from FISMA Audit for Fiscal Year 2024 Report

In the Federal Information Security Act of 2014 (FISMA) audit for fiscal year 2024, CliftonLarsonAllen LLP made 23 recommendations.[40] Of the 23 recommendations, 21 were repeat recommendations from the prior year.[41]

The FISMA audit assesses the VA-wide security management program, and recommendations in the FISMA report are not specific to the VA Beckley Healthcare System. Recommendations 6 and 7 were made to the Office of Personnel Security, Human Resources, and Contract Offices.[42] The other 21 recommendations were made to the assistant secretary for information and technology.

All recommendations are reprinted below:

1. Implement an improved continuous monitoring program in accordance with the National Institute of Standards and Technology's Risk Management Framework. Specifically, regarding the independent evaluation of the effectiveness of security controls prior to granting authorization decisions.
2. Implement improved processes for reviewing and updating key security documentation, including Security Control Assessments, Risk Assessments, and Privacy Impact Assessments as needed. Such updates will ensure all required information is included and accurately reflects the current environment, new security risks, and applicable federal standards.
3. Implement improved processes to ensure System Security Plans reflect the status of security control implementations and risks are accurately reported to support a comprehensive risk management program across the organization.
4. Implement improved mechanisms to ensure system owners and information system security officers follow procedures for establishing, tracking, and updating plan of actions and milestones for all known risks and weaknesses including those identified during security control and other assessments.

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

[41] Recommendations 11 and 16 were new in 2024.

[42] The deputy chief information officer, connectivity and collaboration services, performing the delegable duties of the assistant secretary for information and technology and chief information officer, responded to recommendations 6 and 7.

5. Implement measures to ensure that system stewards and other officials responsible for system-level plans of actions and milestones are closing items with relevant support that shows sufficient remediation of the identified weakness.
6. Strengthen processes to ensure appropriate levels of background investigations are performed timely and completed for applicable VA employees and contractors.
7. Implement improved processes for establishing and maintaining accurate investigation data within VA systems used for background investigations.
8. Ensure contingency plans for all systems and applications are updated and tested in accordance with VA requirements.
9. Implement improved procedures to ensure that system outages are resolved within stated recovery time objectives.
10. Ensure system owners consistently implement processes for periodic reviews of user account access. Remove unnecessary and inactive accounts on systems and networks.
11. Ensure the consistent monitoring and reviewing of privileged accounts, service accounts, and accounts for individuals with access to source code repositories are performed across VA systems and platforms.
12. Implement improved processes to ensure compliance with VA password policy and security configuration baselines on domain controllers, operating systems, databases, applications, and network devices.
13. Ensure established change control procedures are consistently followed for testing and approval of system changes for VA applications and networks.
14. Implement and consistently enforce established procedures for preventing and detecting potential unauthorized changes across all platforms and applications in the environment.
15. Ensure that all systems and platforms are monitored for compliance with documented VA standards for baseline configurations. Ensure that system owners consistently implement and monitor their configurations.
16. Implement automated software management processes on all agency platforms to identify and prevent the use of unauthorized software on agency devices.
17. Implement improved procedures for establishing, documenting, and monitoring an accurate software and logical hardware inventory for system boundaries across the enterprise.
18. Implement improved processes for monitoring and analyzing significant system audit events for unauthorized or unusual activities across all systems and platforms

in accordance with VA policy. Ensure privileged activity is monitored on all systems and applications.

19. Enable system audit logs on all critical systems and platforms and conduct centralized reviews of security violations across the enterprise.
20. Implement improved mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and Web application servers in accordance with established policy time frames. If patches cannot be applied or are unavailable, other protections or mitigations should be documented and implemented to address the specific risks.
21. Implement improved segmentation controls that restrict vulnerable medical devices from unnecessary access from the general network.
22. Implement improved processes to require system owners and management to provide adequate credentials to ensure security scans are authenticated to end devices where feasible and the subsequent vulnerabilities are remediated in a timely manner.
23. Improve the process for tracking and resolving vulnerabilities that cannot be addressed by enterprise processes within policy time frames. Implement mitigations for identified security deficiencies by applying security patches, system software updates, or configuration changes to reduce applicable security risks.

# Appendix C: Additional Background

## Federal Information Security Modernization Act of 2014 (FISMA)

The following are the stated goals of FISMA:

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

FISMA also requires an annual independent assessment of each agency's information security program to determine its effectiveness. Inspectors general or independent external auditors must conduct annual evaluations. The VA Office of Inspector General (OIG) accomplishes the annual FISMA evaluation through a contracted external auditor and oversees the contractor's performance.

## National Institute of Standards and Technology Information Security Guidelines

The National Institute of Standards and Technology (NIST) is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems.[43] NIST develops information security standards and guidelines in

[43] US Department of Commerce, National Institute of Standards and Technology (NIST), Joint Task Force, NIST Special Publication 800-53, rev. 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, September 2020, updated December 10, 2020.

accordance with its statutory responsibilities under FISMA. NIST Special Publication 800-53 provides a catalog of security and privacy controls for information systems and organizations.[44]

## Federal Information System Controls Audit Manual (FISCAM)

The Government Accountability Office developed *FISCAM,* a methodology for evaluating the confidentiality, integrity, and availability of information systems. *FISCAM* groups information categories of similar risks into the following six broad categories: business process controls, security management, access controls, configuration management, separation of duties, and contingency planning.[45] To help auditors evaluate information systems, *FISCAM* aligns control categories with NIST controls.

[44] NIST Special Publication 800-53.

[45] Government Accountability Office, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-24-107026, September 2024.

# Appendix D: VA Management Comments

**Department of Veterans Affairs Memorandum**

Date: September 3, 2025

From: Deputy Chief Information Officer, Connectivity and Collaboration Services, Performing the Delegable Duties of the Assistant Secretary for Information and Technology and Chief Information Officer (005)

Subj: Office of Inspector General Draft Report, Follow-Up Inspection of Information Security at the Beckley Healthcare System in West Virginia (VIEWS 13220272)

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

1. Thank you for the opportunity to review the Office of Inspector General (OIG) draft report, *Follow-Up Inspection of Information Security at the Beckley Healthcare System in West Virginia* (Project Number 2024-03708-AE-0130). The Office of Information and Technology (OIT) submits the attached comments.
2. OIT is committed to ensuring appropriate information security controls are in place at Department of Veterans Affairs (VA) facilities to protect VA systems and data in compliance with federal security guidance.
3. The OIG made five recommendations. VA concurs with recommendations 1-3 and 5. VA provides a corrective action plan and target implementation date for recommendation 1, and closure evidence demonstrating VA has addressed the findings for recommendations 2, 3, and 5. VA non-concurs with recommendation 4.

| |
|---|
| *The OIG removed point of contact information prior to publication.* |

(Original signed by)

Eddie Pool

Attachment

Attachment

**Office of Information and Technology**

**Comments on Office of Inspector General Draft Report,**

Follow-Up Inspection of Information Security at the VA Beckley Healthcare System in West Virginia

Project Number 2024-03708-AE-0130

(VIEWS 13220272)

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

**VA Response:** Concur. The Beckley Department of Veterans Affairs (VA) Medical Center is working with system stakeholders to ensure plans of action and milestones are created for vulnerabilities that cannot be mitigated in accordance with VA timelines.

**Expected Completion Date:** September 30, 2025.

**Recommendation 2: Develop and approve an authorization to operate for the special-purpose systems.**

**VA Response:** Concur. The Special Purpose-Legacy Information Technology Environment (SP-LITE) received an authorization to operate (ATO) in February 2025.

**Expected Completion Date:** Completed February 18, 2025.

VA requests closure of Recommendation 2.

**Recommendation 3: Include system personnel in the security categorization process to ensure all necessary information types are considered when determining the security categorization for special-purpose systems.**

**VA Response:** Concur. The SP-LITE system personnel were included in the security categorization process to ensure that all necessary information types are considered when determining the security categorization for special-purpose systems prior to granting the ATO. The authorization official granted an ATO to the SP-LITE in April 2025.

**Expected Completion Date:** Completed April 2, 2025.

VA requests closure of Recommendation 3.

**Recommendation 4: Segregate [the pharmacy application] administrative access from individuals who are custodians of the pharmaceutical inventory.[46]**

**VA Response:** Non-concur. Pharmacy technicians manage inventory updates primarily to support procurement activities. All activities within [the pharmacy application] are tracked and reportable. Applying the separation of duties requirement to administrator access in [the pharmacy application] would present

[46] 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 OIG removed the name of the pharmacy application.

a challenge because all pharmacy personnel need medication access, making this approach inefficient and inconsistent with management practices.

VA requests closure of Recommendation 4.

**Recommendation 5: Ensure that a witness observes the destruction of temporary paper files that contain personally identifiable information and protected health information.**

**VA Response:** Concur. The Beckley VA Medical Center designated an employee within the Privacy Office to witness the destruction of paper files sent to the shredding vehicle. The Privacy Office will verify the destruction through documentation certifying that the established process was followed.

**Expected Completion Date:** Completed April 4, 2025.

VA requests closure of Recommendation 5.

*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<br>Sachin Bagai<br>Nicholas Hartzheim<br>Kimberly Moss<br>Albert Schmidt |
| **Other Contributors** | Timothy Moorehead<br>Nicholas Neagle<br>Jill Russell<br>Rashiya Washington |

# Report Distribution

## VA Distribution

Office of the Secretary
Office of Accountability and Whistleblower Protection
Office of Congressional and Legislative Affairs
Office of General Counsel
Office of Information and Technology
Office of Public and Intergovernmental Affairs
Veterans Health Administration

## Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Government Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget
US Senate: Jim Justice, Shelley Moore Capito
US House of Representatives: Carol Miller, Riley Moore

**OIG reports are available at www.vaoig.gov.**