US DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

DEPARTMENT OF VETERANS AFFAIRS

Review of Physical Security of Information Technology Equipment at the Columbia, South Carolina, VA Regional Office

Review | 25-04347-110 | June 23, 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) assessed a hotline complaint alleging that hundreds of information technology (IT) devices at the Veterans Benefits Administration regional office in Columbia, South Carolina, were stored in unsecured areas. Leaders and staff at the Columbia VA Health Care System and local staff with the Office of Information and Technology (OIT) are responsible for managing on-site IT equipment.

The OIG examined whether the Columbia VA Regional Office had physical security controls in accordance with federal and VA requirements and standards and whether access to IT equipment was restricted. The team observed during a July 2025 site visit that IT equipment, including laptops and monitors, was stored in unsecured areas. OIT provided evidence in October 2025 that the IT equipment referenced in the allegation and observed on-site by the team had been moved to a secure area. In addition, OIT updated the local inventory procedure in response to the OIG's work. The OIG informed leaders from the Columbia VA Health Care System, the Columbia VA Regional Office, and OIT in December 2025 about the review's preliminary results and recommendations. In March 2026, the OIT End User Operations area manager (OIT manager) showed the team online tools he had developed to better track Columbia's IT equipment.

The OIG made two recommendations to further improve the effectiveness of IT storage and equipment management in the Columbia VA Health Care System. The Columbia VA Health Care System concurred with the recommendations and provided responsive action plans in May 2026.

What the Review Found

The OIG substantiated the allegation that IT equipment was stored in unsecured areas at the Columbia VA Regional Office—contrary to VA Directive 7002, which says access to IT equipment storage locations "will be restricted to authorized IT staff."[1] Additionally, the OIG found that OIT did not effectively manage IT equipment in storage, resulting in unused equipment that was nearing or beyond the end of its useful life expectancy. For the OIG, these findings led to concerns about waste and abuse of taxpayer dollars as well as potential tampering, loss, and theft of government equipment.

The OIG team identified 482 devices—worth $348,293—across three locations relevant to this review. The team excluded expendable IT equipment that cost less than $300. The team found that the OIT manager did not use the most complete IT inventory data when making decisions about using equipment. This occurred because the OIT manager did not integrate federal and VA

[1] VA Directive 7002, *Logistics Management Policy*, January 8, 2020.

requirements for physical security and IT equipment management into local inventory procedures. As a result, Columbia OIT staff did not implement sufficient physical security controls to protect IT devices in a temporary staging area. The review team also determined that

- Columbia OIT staff should have distributed 241 unused IT devices, worth $178,223, before new equipment was purchased, and
- another 82 IT devices in storage, worth $127,384, had not been used and were past their life expectancy.

The OIG found that the taxpayer funds spent on the unused equipment could have been put to better use.

Next Steps

The OIG will monitor the Columbia VA Health Care System's corrective actions and will close the recommendations once officials provide sufficient evidence that they have addressed the risks identified in this report.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

Contents

Abbreviations

IT	information technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information and Technology
VBA	Veterans Benefits Administration

Introduction

The VA Office of Inspector General (OIG) received a hotline complaint in June 2025 that hundreds of information technology (IT) devices—including new laptops and computer monitors—were stored in unsecured areas at the Veterans Benefits Administration (VBA) regional office in Columbia, South Carolina.

To investigate the allegation, the review team examined whether staff implemented physical security controls in accordance with federal and VA requirements. The team also applied National Institute of Standards and Technology (NIST) criteria for evaluating access controls, including physical security. Access controls provide federal agencies with reasonable assurance that computer resources are restricted to authorized individuals.[2]

VA-Wide Equipment Support

The VA Office of Information and Technology (OIT) oversees IT inventory management at the national and local levels. OIT's End User Services, specifically its End User Operations group, manages IT services department-wide, including deploying, activating, and installing IT equipment. At the local level, End User Operations supports IT equipment and software used by VA staff and contractors and is overseen by area managers. This group also maintains or repairs broken IT equipment, provides IT support for new facilities or spaces, and refreshes IT equipment to reduce the number of devices of a certain age.

At the Columbia VA campus, leaders and staff of the Columbia VA Health Care System and local OIT staff are responsible for managing IT equipment.

Equipment Management at the Columbia VA Health Care System

According to VHA Directive 1761, the Columbia VA Health Care System director is responsible for ensuring resources are properly allocated to support the facility's supply chain management program.[3] The directive specifies that the chief supply chain officer oversees the supply chain management program, takes responsibility for inventory, and serves as the facility's accountable official based on VA Handbook 7002, which deals with logistics management procedures.

The director designates one individual from each of the facility's departments as the custodial officer for the property assigned to them.[4] According to VA Directive 7002, the custodial officer certifies that all inventory assigned to them is accounted for as of the date they accept it. At the

[2] NIST, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Revision 5, December 10, 2020.

[3] VHA Directive 1761, *Supply Chain Management Operations*, December 30, 2020.

[4] VA Directive 7002, *Logistics Management Policy*, January 8, 2020.

Columbia VA Health Care System, the director designated the OIT End User Operations area manager (OIT manager) to serve as the custodial officer responsible for managing on-site IT equipment.

IT Equipment Inventory

As the custodial officer, the OIT manager should use Maximo, a web-based equipment management system, to manage equipment and track IT inventory. VA Directive 7002 requires a custodial officer to establish an equipment inventory listing as the inventory record in Maximo for all property assigned to them.[5] These lists capture items, including those that cost over $300—such as VA-owned equipment and equipment, like laptops, loaned to employees.

Columbia staff use the equipment inventory listing to track equipment information, such as the description, serial number, model, location, last inventory date, and purchase price. Staff also use the equipment inventory listing to conduct a physical inventory of equipment at least once a year, as required by VHA Directive 1761.[6] To conduct the inventory, the OIT manager or a delegate must physically scan each item's barcode label or confirm that the equipment recorded on their equipment inventory listing is available. VA Handbook 7002 says that once all items have been inventoried, the OIT manager is required to certify the inventory with a signature in Maximo.[7] Although OIT staff have other ways to monitor IT inventory, such as by using VA dashboards, a system of record like Maximo should be used to track local inventory according to these VA requirements.

IT Equipment Management

According to an OIT standard operating procedure for the Columbia campus, when IT equipment is delivered, designated staff review receiving reports and then tag and scan the equipment into Maximo.[8] They enter the inventory date and update the location field in the system to indicate where the equipment is stored. They then notify an OIT staff member about the delivery and schedule a time to move the equipment elsewhere.

On campus, the OIT staff receive all new IT equipment and software. Once an item has been processed, an IT supervisor notifies facility staff and delivers the equipment. OIT staff pick it up, distribute it within 24 hours, and update Maximo.[9]

[5] VA Directive 7002.

[6] VHA Directive 1761.

[7] VA Handbook 7002, *Logistics Management Procedures*, January 2020.

[8] OIT, "SOP VA Columbia Asset Management Program," SOP: SE-CMS-001, March 16, 2021.

[9] OIT, "SOP VA Columbia Asset Management Program"; Columbia VA Health Care System, William Jennings Bryan Dorn VA Medical Center, "Receiving Non-Expendable Property," 90-31-SOP, June 18, 2024.

Results and Recommendations

Finding: OIT Did Not Effectively Manage IT Equipment at the Columbia Campus

The OIG substantiated the hotline allegation that IT equipment was stored in unsecured areas of the Columbia VA Regional Office. The review team identified almost 500 IT devices, worth $348,293, left in a staging area that was not secured because Columbia OIT staff did not implement sufficient physical security controls to protect IT devices in temporary spaces. This made the items susceptible to tampering, loss, and theft, thereby raising concerns about potential waste and abuse of taxpayer dollars.

While reviewing the allegation, the team also found that the Columbia OIT manager was not using the most complete inventory data to manage local IT equipment. This resulted in unused IT equipment being left in storage for more than half of the items' useful life expectancy and in some cases past their life expectancy altogether. The OIG identified $305,607 worth of unused equipment at locations on the Columbia campus relevant to this review; in some cases, new equipment had been purchased even though the same items were already on-site. The OIG found that the funds from taxpayer dollars spent on the unused equipment could have been put to better use.[10]

What the OIG Did

In July 2025, the OIG team conducted a site visit to the Columbia VA Health Care System campus—including the VBA regional office—and observed the physical security controls for IT equipment in locations relevant to this review. The team reviewed laws, regulations, and related policies and procedures applicable to IT equipment and interviewed OIT and Columbia facility staff. The team also reviewed IT devices in equipment inventory listings and analyzed data from the Maximo system to determine whether equipment was being used. This review included desktop computers, laptops, printers, and high-value monitors (valued above $300). For more on the scope and methodology, see appendix A.

In December 2025, the team briefed leaders in the Columbia VA Health Care System, the Columbia VA Regional Office, and OIT about the report's preliminary results and recommendations.

[10] Appendix B details the monetary benefits identified during this review.

IT Equipment Not Secured

During the site visit, the review team observed IT devices at the VBA regional office that were stored in unsecured areas that had little or no access control. Specifically, the team identified 482 pieces of IT equipment—valued at $348,293—across three locations relevant to this review: two sides of an open office space as well as an unsecured training room. As shown in figure 1, the devices stored in these accessible locations could enable unauthorized staff to tamper with or remove the equipment.

Figure 1. *Unsecured IT equipment at the Columbia VA Regional Office, as seen in July 2025.*
Source: VA OIG staff.

An OIT supervisor reported that, starting sometime in 2023, these areas had served as a staging site to store equipment before it was distributed to new employees and those returning to in-office work. The various IT devices, including laptops, printers, and television monitors, were stacked in boxes or on pallets or carts.

VA Directive 7002 references NIST standards and says access to IT equipment storage locations "will be restricted to authorized IT staff."[11] The directive says IT equipment storage locations must be physically secured under the same guidelines that NIST Special Publication 800-53 establishes for computer rooms. NIST explains that agencies must

- maintain physical control over output devices, including room-level access restrictions and monitoring;

[11] VA Directive 7002.

- monitor physical entry points to prevent and detect unauthorized access; and
- ensure sensitive IT equipment is in secure areas.[12]

The review team observed that the regional office has an x-ray machine, a metal detector, and guards at its front entrance. However, the team confirmed that while the office had badge access and camera surveillance in some areas, the staging area the team observed lacked camera surveillance and had no locked doors. About 150 non-IT VA staff had office space near the staging area, yet access to the stored equipment was not restricted. Without sufficient physical security controls to protect the IT devices, Columbia OIT staff risked equipment being tampered with, stolen, or lost.

In October 2025, the OIT manager provided evidence that the IT equipment was no longer in the staging area that the review team had observed. The manager reported that the equipment had instead been moved to a secure location.

Incomplete Inventory Reports and Unused Equipment

The review team learned that the OIT manager mainly used reports from three internal VA dashboards to track IT equipment rather than the data from Maximo, Columbia's inventory system of record. The reports from these dashboards provide information on the status of equipment, including the number of online laptops and desktop computers—but the team determined that the reports included only a fraction of warehouse assets rather than a comprehensive list. For example, on December 11, 2025, the dashboards listed 11,989 items with 145 of them in storage; that same day, Maximo data showed 23,572 IT items with 1,418 in storage. An OIT End User Services director explained that reports from the dashboards would not identify devices unless they had been on VA's network and detected. The OIG determined that nonactive devices were the cause of the discrepancy between the internal dashboards and Maximo records.

The OIT manager's reliance on the three internal VA dashboards resulted in devices being left in storage and not used for more than half their expected life. OIT guidance dictates the life expectancy of equipment by type; for example, a desktop computer is expected to last four years, a laptop three.[13] Notably, the review team identified 82 IT devices worth $127,384 that were past their life expectancy.

In addition, according to Maximo data, 588 devices in the warehouse and 39 devices in the regional office were more than halfway through their life expectancy as defined by OIT. According to 41 C.F.R. § 102-36.35 (2000), existing VA property must, to the maximum extent practicable, be used before purchasing new property. The OIG team determined that the

[12] NIST Special Publication 800-53.

[13] OIT, *Life Expectancy (LE) Updates for OIT Category Stock Numbers (CSNs)*, March 12, 2025.

$178,223 spent on 241 of these IT devices already on-site could have been put to better use before purchasing new equipment. OIT missed the opportunity to distribute this equipment in a timely manner and consistent with federal regulations. The OIG determined that the value of *all* unused equipment the team identified for this review was $305,607.[14] VA could have put these funds to better use.

According to Maximo data, 540 IT devices yet to be distributed at the Columbia warehouse as of November 2025 were at least halfway through their OIT life expectancy—a decrease from 588 devices in July. In addition, 121 unused items in storage were past the end of their useful life expectancy, an increase from 82 identified in July.

The OIG concluded that, because Columbia OIT did not use complete IT inventory data, the OIT manager did not know that some items in storage were near or beyond their life expectancy and should have been used. Ultimately, this situation raised concerns about potential waste and abuse of taxpayer dollars.

Inventory Management Procedures

The OIG determined that the Columbia OIT did not integrate federal and VA requirements related to the physical security and management of IT equipment into local inventory procedures.

The OIT manager and other VA staff said the Columbia OIT's security procedures were acceptable because employees in the building were vetted by VA and the building was not accessible to the public. However, in addition to federal and VA requirements to maintain physical control over IT devices, VA Handbook 0730/4 requires controls for temporary storage and staging areas.[15] The OIG found that, despite this guidance, both the March 2021 and the December 2025 local OIT inventory procedures did not specify what the practice should be when temporary IT storage space is used.[16]

In addition, the Columbia OIT inventory procedures did not require staff to consider unused equipment when managing IT inventory.[17] Specifically, the procedures were silent on which information sources and methodology should be used to make decisions about the number of IT devices that need to be replaced, refreshed, or activated.

The procedures also did not provide steps about how staff should use equipment on a first-in, first-out basis. This practice, which aligns with 41 C.F.R. § 102-36.35, is used in inventory management to ensure the first items entering an inventory are the first ones to leave when it is

[14] Appendix B provides more information on the monetary benefits identified during this review.

[15] VA Handbook 0730/4, *Security and Law Enforcement*, March 2013.

[16] OIT, "SOP VA Columbia Asset Management Program"; OIT, "SOP Area Columbia SC Asset Management Program," SOP: SE-CMS-001, December 10, 2025.

[17] OIT, "SOP VA Columbia Asset Management Program"; OIT, "SOP Area Columbia SC Asset Management Program."

time for them to be used. An OIT End User Services director agreed that first-in, first-out is a best practice to manage inventory.

In response to the OIG's work, the OIT manager updated the local inventory procedure in December 2025. In March 2026, the manager demonstrated for the review team the online tools he had developed to better track IT equipment at the Columbia campus.

While these improvements are important, Columbia OIT and facility staff should take additional steps, such as updating the IT inventory procedure to include contingencies for securing equipment when temporary space is needed and ensuring all equipment is used according to requirements. Additionally, because the process for monitoring IT inventory at the Columbia VA Health Care System may not include all unused equipment, OIT and facility staff should conduct an on-site assessment of all IT assets and take action as needed.

Conclusion

The OIG substantiated the hotline allegation that IT equipment was not stored appropriately at the Columbia VA Regional Office. During its July 2025 site visit, the review team determined that 482 pieces of IT equipment, worth $348,293, were not secured. Although OIT staff moved the equipment to a secure location after the team's visit, VA staff must remain vigilant to ensure IT equipment is protected from tampering, loss, and theft and to prevent the potential waste and abuse of taxpayer dollars.

The OIG also determined that the local OIT office did not properly manage aging and unused IT equipment. The team determined that 82 IT devices, worth $127,384, had not been used and were past their useful life expectancy. OIT also should have distributed 241 unused IT devices, worth $178,223, before new equipment was brought on-site. Because the OIT manager did not use complete information for IT inventory, he could not accurately determine what was available for campus staff. Overall, the OIG found that VA could have put these taxpayer funds to better use for the department and the veterans it serves.

Recommendations 1–2

The OIG made the following recommendations to the Columbia VA Health Care System director, the facility's chief supply chain officer, and the OIT area manager:[18]

1. Update the local inventory procedure to include a process for securing information technology equipment when temporary space is needed and for tracking and distributing this equipment, in accordance with federal and VA requirements.

[18] The recommendations addressed to the director of the Columbia VA Health Care System are directed to anyone in an acting status or performing the delegable duties of the position.

2. Assess the age of all unused information technology inventory to determine what should be used and what should be disposed of based on federal and VA requirements, and take action to address the results.

VA Management Comments

In April and May 2026, the Veterans Integrated Service Network 7 acting director and the Columbia VA Health Care System acting executive director both concurred with the OIG's findings. The acting executive director of the facility concurred with recommendations 1 and 2 and provided action plans for each. Appendixes C and D include the full text of VA's comments.

For recommendation 1, the facility acting executive director expressed commitment to compliance with the facility's local procedure regarding controls to receive, barcode, inventory, inspect, and store IT equipment. The director reported that unsecured staging areas were eliminated and that only badge access–controlled storage locations are permitted. He also stated that all IT equipment will be moved to the designated OIT secure storage area upon receipt. The facility reported that all IT equipment will be processed, barcoded, and recorded in a timely manner.

To address recommendation 2, the facility acting executive director reported that the facility will ensure all IT inventory is accurately maintained and documented in Maximo, including acquisition dates and statuses. He stated that periodic reviews of inventory records will be conducted to identify unused equipment and assess its age. He further noted that appropriate actions will be taken, such as reintegrating items into use as needed or properly disposing of items using established processes.

OIG Response

The Columbia VA Health Care System provided responsive action plans with target completion dates for recommendations 1 and 2. The OIG will monitor implementation of the planned actions for both recommendations. The OIG will consider them open until VA has provided sufficient evidence to demonstrate that corrective actions have been implemented.

Appendix A: Scope and Methodology

Scope

The VA Office of Inspector General (OIG) received a hotline complaint in June 2025 concerning information technology (IT) equipment storage at the Columbia VA Regional Office. The review team conducted a site visit to the Columbia VA Health Care System in July 2025 for an initial assessment and performed this review from November 2025 through April 2026. The review scope included an assessment of physical security controls at the regional office at the time of the OIG's site visit. While investigating the allegation, the team also visited the Columbia VA warehouse. Throughout the review period, the team considered any applicable developments, such as updates to local inventory procedures.

Methodology

To accomplish the objective, the OIG examined relevant federal law and regulations, VA policy and procedures, and National Institute of Standards and Technology security guidelines. In July 2025, the review team inspected IT equipment at various locations on the Columbia campus relevant to this review and the hotline allegation. In addition, the team interviewed VA staff responsible for IT physical security and equipment management at the Columbia VA Health Care System—including from VA's Office of Information and Technology, the regional office, and the supply chain management service.

After the site visit, the team assessed the management of IT equipment at the locations relevant to this review and analyzed Maximo data. Specifically, the team analyzed VA inventory data from July, November, and December 2025. These data were obtained using Maximo system access through the VA Corporate Data Warehouse and were used to determine the number of operational IT devices at the locations relevant to the review, as well as the age and purchase price of the equipment.

The team focused its analysis on VA equipment inventory listings (780, 780P, 78YM, and 78Z2) for IT devices, such as laptops, desktop computers, printers, and monitors; the team excluded expendable IT equipment that cost less than $300. The team used the data to identify items kept in storage. Last, the team calculated the age of the IT inventory in storage using the Maximo installation date and compared Maximo data to reports from three VA dashboards. The team assessed the results of its data analysis, interviews, and inspection to identify any relevant noncompliance.

Internal Controls

The review team assessed internal controls to determine whether they were significant to the objective. This included consideration of the five internal control components: control

environment, risk assessment, control activities, information and communication, and monitoring.[19] In addition, the team reviewed the principles of internal controls as associated with the objective and identified one component and two principles as significant.[20] The team identified internal control deficiencies during this review and proposed recommendations to address those listed in table A.1.

Table A.1. VA OIG Analysis of Internal Control Components and Principles Identified as Deficient

Component	Principle	Deficiency identified by this review
Control activities	10. Management should design control activities to achieve objectives and respond to risks.	The Columbia Office of Information and Technology did not adequately assess the age of IT equipment, which affected staff's ability to accurately determine the amount of equipment needed.
	12. Management should implement control activities through policies.	The Columbia Office of Information and Technology lacked procedures that addressed the temporary storage and management of IT equipment on campus.

Source: VA OIG analysis of internal control components and principles. The principles listed are consistent with the Government Accountability Office's Standards for Internal Control in the Federal Government.

Data Reliability

The OIG obtained inventory data for IT equipment from Maximo to identify the number of devices—including their age and purchase price—in the regional office and in the campus warehouse. The review team researched Maximo and its data by reviewing VA documentation, which provided information about the data tracked in the system, and by interviewing VA staff.

To ensure the reliability of computer-processed data, the team conducted multiple reasonableness tests of Maximo data to verify the quality of the data used during the review. The team also conducted other tests of these data, including a comparison of the data collected while counting the IT equipment in the Columbia VA Regional Office to extracted data from Maximo in July 2025. In addition, the team compared fields from extracted Maximo data from three different dates in July 2025 to purchase-order data from September 2025 from the Integrated Funds Distribution Control Point Activity, Accounting, and Procurement system (a data repository). The team also compared purchase-order shipment documentation for IT equipment shipped to the Columbia VA Health Care System to six data fields in the Maximo data from

[19] Government Accountability Office (GAO), *Standards for Internal Control in the Federal Government*, GAO-14-704G, September 2014.

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

July 2025. Finally, the team took data from three fields in the equipment inventory listings of IT devices identified in the Columbia warehouse in July 2025. The team compared these fields to two different extracted datasets from Maximo obtained in August and September 2025. Based on these reliability assessments, the team concluded that the Maximo inventory data used during the review were appropriate and sufficient.

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*.[21]

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

Appendix B: Monetary Benefits in Accordance with Inspector General Act Amendments

Recommendations	Explanation of Benefits	Better Use of Funds[22]	Questioned Costs
1–2	Two hundred and forty-one information technology devices could have been used before new equipment was purchased.	$178,223	$0
1–2	Eighty-two unused information technology devices in storage had not been used and were beyond their life expectancy.	$127,384	$0
	Total	**$305,607**	**$0**

[22] The IG Act defines "better use of funds" as a recommendation by the project team that funds could be used more efficiently if management took actions to implement and complete the recommendation. This includes (1) implementing recommended improvements that would result in not incurring costs related to the operations of the establishment, a contractor, or grantee, or (2) as any other savings that are specifically identified.

Appendix C: VA Management Comments, Acting Director, Veterans Integrated Service Network 7 (VISN 7) Southeast Network

Department of Veterans Affairs Memorandum

Date: May 15, 2026

From: Acting Director, Department of Veterans Affairs (VA) Veterans Integrated Service Network 7 (VISN 7) Southeast Network (10N7)

Subj: Review of Physical Security of Information Technology Equipment at Columbia, South Carolina, Regional Office

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

1. We appreciate the opportunity to review and comment on the OIG draft report, Review of Physical Security of Information Technology Equipment at Columbia, South Carolina, Regional Office. I have completed a full review of the draft report and concur with the findings. We are committed to ensuring Veterans receive quality care that utilizes the high-reliability pillars, principles, and values.
2. I have reviewed the documentation and concur with the response as submitted.
3. I appreciate the opportunity for this review as part of a continuing process to improve the care of our Veterans.

The OIG removed point of contact information prior to publication.

(Original signed by)

Benita K. Miller, FACHE, LISW-CP

Attachment

Appendix D: VA Management Comments, Acting Executive Director/CEO, Columbia VA Health Care System

Department of Veterans Affairs Memorandum

Date: April 28, 2026

From: Acting Executive Director/ CEO, Columbia VA Health Care System (544/00)

Subj: Review of Physical Security of Information Technology Equipment at Columbia, South Carolina, VA Regional Office

To: Director, Southeast Network (10N7)

1. The Columbia VA Health Care System would like to thank the Office of the Inspector General Team for the thorough review and assessment during the Review of Physical Security of Information Technology Equipment at Columbia, South Carolina, VA Regional Office.
2. I have reviewed each recommendation and concur with the findings, recommendations and submitted action plans. The plans have been carefully analyzed and will be implemented and monitored through satisfactory completion.

(Original signed by)

Jeffrey Soots

Acting Executive Director/ CEO

Columbia VA Health Care System

Attachment

Attachment

Recommendation 1

1.Update the local inventory procedure to include a process for securing information technology equipment when temporary space is needed and for tracking and distributing this equipment, in accordance with federal and VA requirements.

Healthcare system concurred.

Target date for completion: 7/19/2026

Healthcare system response: The Columbia VA Health Care System is committed to full compliance with local Standard Operating Procedure (SOP) 90-31, which establishes comprehensive controls for the receiving, barcoding, inventory entry (via Maximo), inspection, and secured storage of IT equipment. In alignment with SOP 90-31:

All IT equipment will be processed and barcoded within 1 working day of receipt and recorded in Maximo within 5 days. Upon receipt, all IT equipment will be moved immediately to the designated OI&T secured storage area (Building 7 Warehouse), with access strictly limited to authorized OI&T and Supply Chain personnel. Open or unsecured staging areas have been eliminated; only badge-access controlled storage locations are permitted. If temporary storage is required, it must be badge-access controlled, logged in Maximo as a temporary location, and assigned appropriate custodial accountability.

OI&T retains sole responsibility for the distribution and issuance of GFE/IT equipment. Supply Chain Management (SCM) will continue to support accountability and oversight functions through the execution of the 13-month accountability SCCOP report, identification and notification to OI&T of assets not inventoried within required timeframes and the initiation and tracking of Reports of Survey (ROS) for unaccounted equipment until resolution (located or formally written off).

Through expanded enforcement and operationalization of these procedures, the Columbia VA Health Care System has addressed and closed the gap identified by the OIG regarding the securing, tracking, and distribution of IT equipment, including scenarios requiring temporary storage.

This action plan will be tracked through local governance via the Columbia VA Health Care System Continued Survey Readiness Committee.

Recommendation 2

2. Assess the age of all unused information technology inventory to determine what should be used and what should be disposed of based on federal and VA requirements and take action to address the results

Healthcare system concurred.

Target date for completion: 7/19/2026

Healthcare system response: The Columbia VA Health Care System will ensure that all IT inventory is accurately maintained and documented in Maximo, including acquisition dates and current status (e.g., active, temporary storage). Regular, periodic reviews of inventory records will be conducted to identify unused equipment and assess its age. Any IT equipment identified as unused and exceeding federally or VA-defined age thresholds will be flagged for further evaluation. In compliance with VA and federal guidelines, appropriate actions will be taken, such items will either be reintegrated into active use as needed or properly disposed of through established disposal processes.

These measures will ensure proactive assessment of IT inventory age and usability, and demonstrate the facility's commitment to meeting OIG requirements for effective management and disposition of IT assets.

This action plan will be tracked through local governance via the Columbia VA Health Care System Continued Survey Readiness Committee.

The text of VA's management comments is reprinted verbatim as received from the department. 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.
Review Team	Jessica Blake, Director Benjamin Howe Ibrahim Kadara Nicolas Shands Amanda Taylor
Other Contributors	Georgina Baumgartner Victor Rhee Rashiya Washington

Report Distribution

VA Distribution

Office of the Secretary
Office of Accountability and Whistleblower Protection
Office of Congressional and Legislative Affairs
Office of General Counsel
Office of Information and Technology
Office of Public and Intergovernmental Affairs
VISN 7: VA Southeast Network
Columbia VA Health Care System

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Government Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget
US Senate: Lindsey Graham, Tim Scott
US House of Representatives: Sheri Biggs, Jim Clyburn, Russell Fry, Nancy Mace, Ralph Norman, William Timmons, and Joe Wilson

OIG reports are available at vaoig.gov.