NATIONAL
ARCHIVES

OFFICE *of* INSPECTOR GENERAL

Evaluation of NARA's Information Technology Inventory (26-R-03)

February 25, 2026

NATIONAL
ARCHIVES

Inspector General

February 25, 2026

TO: Valorie Findlater
Chief of Management and Administration

FROM: William Brown
Acting Inspector General

SUBJECT: *Evaluation of NARA's Information Technology Inventory*
OIG Report No. 26-R-03

Attached is the Office of Inspector General's final evaluation report for the subject engagement. The report contains ten recommendations made to strengthen management and internal controls over NARA's IT inventory. Agency staff indicated they had no comments for inclusion in the report.

Please provide planned corrective actions and expected dates to complete the actions for each of the recommendations within 30 days of the date of this report. As with all OIG products, we determine what information is publicly posted on our website from the published report. Consistent with our responsibility under the Inspector General Act of 1978, as amended, we may provide copies of our report to congressional committees with oversight responsibility for NARA.

We appreciate the cooperation and assistance NARA extended to us during this evaluation. Please contact me with any questions.

Table of Contents

Executive Summary

Evaluation of NARA's Information Technology Inventory

OIG Report No. 26-R-03 February 25, 2026

Why Did We Conduct This Evaluation?

The National Archives and Records Administration (NARA) manages a wide range of government-issued information technology (IT) assets. Recent workforce transitions have increased the risk that assets may be misappropriated.

The Office of Inspector General (OIG) conducted this evaluation to assess the completeness and accuracy of NARA's IT inventory and determine if adequate policies and procedures are in place to track IT assets.

What Did We Recommend?

We made ten recommendations to strengthen management and internal controls over NARA's IT inventory.

What Did We Find?

NARA's internal controls over information technology assets are not operating effectively. The system that Information Services uses to track IT assets contains data that is incomplete and inaccurate. Thousands of records in the system are missing asset tags, user assignments, and location information. Former employees are still listed as having assigned assets. These data quality issues originate from the transition of a previous NARA contractor. While NARA has taken some steps to improve inventory accuracy, such as physical inventories and surveys of employees, the system cannot currently be relied upon as a complete and accurate source of data on the agency's IT assets.

We also found that several key responsibilities outlined in NARA policy and federal guidance are not being fulfilled. Property Accountable Officers (PAOs) are not receiving their required annual training, and government-issued cell phones are not designated in policy as sensitive personal property. Information Services is not performing monthly reconciliations between employee separation records and asset data, which limits NARA's ability to confirm that equipment is returned when employees leave the agency. Further, Information Services is not transferring assets to the PAOs of end users, preventing those PAOs from effectively overseeing the assets in their own offices. This reduces accountability for the assets and increases the risk of property misappropriation.

Background

The National Archives and Records Administration (NARA) is responsible for ensuring the accountability and stewardship of government property, including information technology (IT) assets. These assets range from laptops and mobile devices to servers that support critical operations across the agency, and must be managed through their full lifecycle, from acquisition to disposal.

NARA Directive 600, *Managing Government Personal Property,* and its Supplement, *NARA Government Personal Property Operating Guide*, outlines the policy and procedures for managing government personal property. Responsibility for managing IT assets at NARA is shared across multiple offices. The Facility & Property Management Division (BF) within Business Support Services is responsible for tracking all of NARA's accountable personal property. BF manages the tracking of accountable personal property using enterprise asset management software. Accountable personal property is defined as personal property that is in the interest of the Government to maintain and ensure proper use, maintenance, and protection beginning with receipt of the property through its disposal. Accountable personal property required to be maintained is as follows:

1. Capitalized personal property;
2. Equipment having a unit cost of $3,000 or more;
3. Borrowed or leased personal property;
4. Sensitive items; and
5. Property belonging to the Government that is in the possession or under the control of contractors.

The End-User Services Branch (IOS) within Information Services manages the issuance, tracking, and documentation of IT assets[1] using a separate software, within which tracking occurs in the Hardware Asset Management (HAM) module. There is substantial overlap in the assets tracked by BF and IOS.

Each organizational unit designates Property Accountable Officers (PAOs) to ensure compliance with personal property management policies. PAOs are charged with maintaining physical custody of assets within their jurisdiction, tracking their assignment and location, and overseeing compliance with property management policies. In most instances, being a PAO is a collateral responsibility that an employee performs within their NARA office. They may also be held financially liable should such property be lost or damaged.

[1] Includes accountable personal property and non-accountable personal property.

Evaluation Results

Finding 1. The Hardware Asset Management Module (HAM) that Information Services Utilizes to Track IT Inventory Contains Inaccurate and Unreliable Data

The End-User Services Branch within Information Services uses the HAM module to track IT equipment across NARA. We found the HAM module contains numerous inaccuracies and inconsistencies. NARA did not establish a process to ensure that data transferred from a contractor was accurate and complete. The Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government*, Principle 13, requires management to use quality information from reliable sources to achieve objectives. Additionally, the National Institute of Standards and Technology (NIST), emphasizes the need to maintain a complete and accurate inventory system. Despite efforts to improve the accuracy and reliability of Information Services' records of IT assets, the HAM module cannot be relied upon. This undermines NARA's ability to ensure accountability over government property, creates inefficiencies for staff attempting to reconcile asset data, and increases the risk of loss, misuse, or untracked disposal of IT equipment.

HAM Review

The OIG reviewed a full export of the HAM module, which contained over 25,000 asset records. The data included numerous blank or inconsistent fields that called into question the reliability of the data. For example, over 2,500 records were missing asset tags in the system, which are the unique identifiers that are critical for tracking physical devices. More than 19,000 assets, 78% of all asset records, lacked a value in the "assigned to" field, which typically reflects the end-user responsible for the asset.

The OIG also identified records still assigned to former agency employees, as well as the presence of virtual machine instances which are non-physical assets that, according to a NARA official should not be included in the HAM.

Prior NITTSS Contractor

A previous NARA Information Technology and Telecommunication Support Services (NITTSS) contractor's engagement ended in 2022, and the contractor did not provide a complete or accurate export of IT asset data to the agency. NARA did not establish a timely process to ensure that the data they injected from the contractor's software instance was accurate or complete[2]. As a result, NARA's IT asset data was populated with incomplete and inconsistent records.

NARA has undertaken efforts to improve data quality. These include conducting physical inventories, asking staff to submit device information through a survey, and tracking asset tags during equipment replacements. However, despite these efforts, the data remains incomplete.

NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Revision 5, September 2020 (includes updates as of Dec. 10, 2020), CM - 8 System Component Inventory, requires federal agencies to develop and document an inventory of information system components that is accurate, prevents duplicate entries, is regularly updated and reviewed, and include relevant information. Further, the *Standards for Internal Control in the Federal Government*, requires management to use quality information from reliable sources to achieve objectives.

The HAM module cannot be relied on as a complete or accurate record of NARA's IT assets. This undermines NARA's ability to ensure accountability over government property, creates inefficiencies for staff attempting to reconcile asset data, and increases the risk of loss, misuse, or untracked disposal of IT equipment.

Recommendations

We recommend the Chief Information Officer:

Recommendation 1: Conduct a full reconciliation of IT inventory records to ensure all assets are accurately documented and assigned.

Recommendation 2: Digitize all IT asset tracking forms and enable electronic submission by end-users and PAOs.

Recommendation 3: Implement an IT asset management lifecycle approach that documents the complete transaction history of an IT asset from its acquisition to its excess from service.

[2] According to a NARA official, as a result of this experience, the agency has acquired its own instance of the software and NITTSS contractors will no longer need to bring their own instance.

Finding 2. Information Services Has Not Been Conducting Monthly Reconciliations of Employee Exit Clearance Reports and Data in Their Tracking System

When employees separate from NARA, it is essential to ensure that all government issued IT equipment is returned and properly documented. Information Services has not been conducting reconciliations of employee exit clearance reports they receive that contain information regarding a NARA employee's separation from the agency with asset return data. The OIG found that the Asset Management Standard Operating Procedure (SOP) does not contain procedures for monthly reconciliations. The *Standards for Internal Control in the Federal Government* underline the need for controls to be properly designed to ensure directives are followed. Information Services may be unaware if a NARA employee separating from the agency has returned all of their IT assets or their assets may be misclassified in the HAM.

Exit Clearance

NARA requires the completion of an electronic exit clearance form be filled out by a departing employee or their supervisor[3]. Completion of the form triggers a notification email sent to the IT Help Desk who creates a ticket in their tracking system to ensure that the employees' equipment is returned. One of the key controls associated with this process is a monthly reconciliation of the exit clearance reports with asset records. The reconciliations are intended to confirm that all equipment assigned to separated employees has been accounted for and updated in the system.

In response to a request for a copy of monthly reconciliations that occurred from January – April 2025, NARA officials acknowledged that the reconciliations had not been performed by the vendor but planned to incorporate the activity by September 1, 2025. Based on interviews with Information Services staff and a review of the Asset Management SOP, OIG determined that there is no documented process for performing these monthly reconciliations.

The *Standards for Internal Control in the Federal Government*, Principle 10, emphasizes the need to design control activities to achieve the organization's objectives. Principle 12 further requires management document in policies for each unit its responsibility for an operational process's objectives and related risks.

The lack of a documented procedure has contributed to the procedure not being performed. Although Information Services has access to the employee exit clearance data and updates IT

[3] The electronic exit clearance form applies to all NARA employees, contractors, volunteers, and interns who separate from NARA or are reassigned to a different NARA organization or location; all separating agency declassification reviewers (Federal employees and contractors); and any separating Foundation employees, contractors, and volunteers who have access to NARA facilities and property.

asset records, a contractor has not been tasked with routinely comparing the two sources to verify whether equipment was returned.

Without routine reconciliations between exit records and inventory data, NARA may be unaware if employees who have separated from NARA failed to return their assigned IT assets. This limits the agency's ability to enforce accountability and maintain accurate inventory records.

Recommendations

We recommend the Chief Information Officer:

Recommendation 4: Expeditiously conduct a reconciliation of IT asset records for employees who have separated from NARA since January 1, 2025, or who remain on administrative leave awaiting separation.

Recommendation 5: Revise the Asset Management SOP to include procedures for conducting a monthly reconciliation of employee exit clearance reports to asset return data and ensure monthly reconciliations are performed.

Finding 3. Information Services is Not Transferring IT Assets to the Proper PAOs

PAOs are responsible for tracking personal property within their jurisdiction, ensuring physical control of assets, and maintaining asset records. Under NARA Directive 600, PAOs are expected to monitor asset assignments, maintain accurate records, and enforce accountability among employees to whom assets are issued. Information Services, a PAO, is responsible for issuing IT assets, but when those assets are deployed to end-users, they are not reassigning them to the appropriate PAO. Information Services found it simpler not to move assets to the PAOs of end-users. Further, Information Services responsibilities are not clearly defined in NARA Directive 600. As a result, IT equipment remains under Information Services' PAO codes, reducing visibility for the PAOs who are best positioned to ensure proper stewardship of those assets.

Assets Not Transferred to the Appropriate PAOs

When Information Services issues an IT asset to a NARA employee, the asset should be reassigned from Information Services' PAO to the PAO corresponding to the employee's organizational unit. This transfer allows the PAO in that unit to monitor the asset and maintain accountability in accordance with NARA Directive 600.

The OIG found that Information Services is not transferring assets to the PAOs of the employees receiving them. Instead, the assets remain listed under one of Information Services' PAO codes. This practice is taking place at Archives I, Archives II, the National Personnel Records Center (NPRC), and the Allegany Ballistics Laboratory (ABL).

During interviews, Information Services staff stated that they found it simpler to retain assets under its own PAO codes. This practice is inconsistent with the intent and requirements of NARA Directive 600, which emphasizes the importance of PAOs being within the same office as the end-users to be able to monitor asset use and ensure compliance due to their regular interaction with the end-users. The OIG also found that NARA Directive 600 did not clearly define Information Services responsibilities. Without transferring assets to the correct PAO, those PAOs cannot effectively oversee the assets within their unit, nor can they take action if equipment is lost or mishandled.

Recommendations

We recommend the Chief Information Officer:

Recommendation 6: Ensure that when IT assets are deployed to end-users those assets are moved from Information Services' PAO codes to the respective PAOs for the end-users as outlined in NARA Directive 600 and the Supplement to Directive 600.

We recommend the Executive for Business Support Services:

Recommendation 7: Revise NARA Directive 600 to reflect current organizational responsibilities.

Finding 4. Government-Issued Cell Phones are Not Tracked by NARA as Sensitive Personal-Property

NARA is required to maintain accountability for sensitive personal property in accordance with federal property regulations. We found that NARA does not track government-issued cell phones as sensitive personal property. NARA's supplement to NARA Directive 600 does not reflect Federal guidance on sensitive property classifications. The General Services Administration (GSA) defines sensitive personal property in 41 Code of Federal Regulations (CFR) § 102-35.20 to include information technology equipment with memory capability and communications equipment, regardless of dollar value. By not classifying or tracking cell phones as sensitive personal property, NARA may be increasing the risk of loss, theft, or unauthorized use of these devices.

Sensitive Personal Property

The supplement to NARA Directive 600 outlines which categories of personal property are considered sensitive property. The OIG found that government issued cell phones are not designated as sensitive personal property in the supplement to NARA Directive 600 and are specifically excluded.

GSA defines sensitive property to include information technology equipment with memory capability and communications equipment, regardless of dollar value. Sensitive personal property is expected to be subject to enhanced accountability and oversight.

Information Services is currently responsible for issuing and tracking mobile phones and maintains those records in the HAM. Although the devices are functionally tracked, they are not formally recognized in policy as requiring special controls and therefore may not receive the same level of scrutiny or protection as other sensitive items. NARA's supplement to NARA Directive 600 has not been updated to reflect Federal guidance on sensitive personal property. As a result, these devices are excluded from the formal policy structure that governs the control of sensitive items, potentially increasing the risk that these assets are misappropriated.

Recommendation

We recommend the Executive for Business Support Services:

Recommendation 8: Revise the Supplement to NARA Directive 600 to align with Federal regulations by designating government-issued cell phones as sensitive personal property.

Finding 5. NARA's PAOs Are Not Receiving Required Annual Training for Managing Government Personal Property

BF has not published personal property management training for PAOs in NARA's Learning Management System (LMS) or established an annual recertification process. NARA Directive 600, requires BF to publish annual training for PAOs and property custodians[4] in the LMS. The directive also places responsibility on executives, staff directors, and other designated officials to ensure PAOs and custodians complete the training and annual recertification. NARA Directive 600 has not been updated since 2012 and does not reflect current practices or expectations. Without consistent, timely, or sufficient training, PAOs may not perform their property management responsibilities.

Annual Training and Recertification

The role of a PAO is usually a collateral responsibility that an employee performs within their NARA office. They are charged with maintaining physical custody of assets within their jurisdiction, tracking their assignment and location, and overseeing compliance with property management policies. This includes completing and retaining various NARA forms for when assets are transferred to another PAO, between end-users, and specific forms for when IT assets are involved. They may also be held financially liable should such property be lost or damaged.

The *Standards for Internal Control in the Federal Government*, Principle 4, emphasizes that management establishes expectations of competence which is largely obtained from professional experience and training. Providing timely, recurring training, and a recertification process helps ensure that PAOs have the necessary knowledge to meet their responsibilities. Without training, PAOs may not be able to fulfill their complex roles ensuring property management policies are followed.

Recommendations

We recommend that the Executive for Business Support Services:

> **Recommendation 9:** Develop and implement standard operating procedures to ensure annual PAO training is created and made available to all relevant staff.
>
> **Recommendation 10:** Track training completion to ensure PAOs and property custodians meet the annual recertification requirement outlined in NARA Directive 600.

[4] Property custodians can be designated by a PAO to assist in the managing of personal property within their assigned area of responsibility.

Appendix A – Objective, Scope, and Methodology

Objective

The objective of this evaluation was to assess the completeness and accuracy of NARA's information technology (IT) inventory and determine if adequate policies and procedures are in place to track IT assets.

Scope and Methodology

To accomplish our objective, we performed evaluation procedures at Archives I in Washington, D.C. and Archives II in College Park, Maryland from March 2025 to August 2025. The scope of the evaluation included IT accountable and non-accountable personal property.

NARA underwent a reorganization effective September 21, 2025. This report utilizes office terminology from prior to the reorganization date, as the associated fieldwork had already commenced.

We performed the following:

- Reviewed relevant guidance:
    - Public Law 115 - 419 - *Federal Personal Property Management Act of 2018*.
    - Title 40 United States Code (U.S.C.) § 524 (2025).
    - 41 CFR § 102-35.20 - What definitions apply to GSA's personal property regulations?
    - OMB Circular A-130, *Managing Information as a Strategic Resource*, issued July 28, 2016.
    - GAO *Standards for Internal Control in the Federal Government* (GAO-14-704G), issued September 2014.
    - National Institute of Standards and Technology (NIST), Special Publication 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* issued September 2020 (includes updates as of Dec. 10, 2020).
    - NARA Directive 600, *Managing Government Personal Property*, issued September 25, 2012.
    - Supplement to NARA Directive 600, *NARA Government Personal Property Operating Guide,* issued September 25, 2012.

  - Information Services, Service Operations Delivery Division, *Asset Management Standard Operating Procedure*, issued December 2024.

- Reviewed data exported from the inventory tracking systems of Business Support Services and Information Services and assessed the completeness, accuracy, and reliability of asset data.
- Reviewed outstanding issues and recommendations relevant to our evaluation objectives, which were identified in previous audits and evaluations.
- Conducted interviews with employees from Information Services and Business Support Services.

The OIG conducted this evaluation in accordance with the *Quality Standards for Inspection and Evaluation* as issued by the Council of the Inspectors General on Integrity and Efficiency (December 2020).

Appendix B – Acronyms

Acronym	Definition
ABL	Allegany Ballistics Laboratory
BF	Facility & Property Management Division
CFR	Code of Federal Regulations
GAO	Government Accountability Office
GSA	General Services Administration
HAM	Hardware Asset Module
IOS	End-User Services Branch
IT	Information Technology
LMS	Learning Management System
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NITTSS	NARA Information Technology and Telecommunication Support Services
NPRC	National Personnel Records Center
OIG	Office of Inspector General
PAO	Property Accountable Officer
SOP	Standard Operating Procedure
U.S.C	United States Code

OIG Hotline

The OIG Hotline provides a confidential channel for reporting fraud, waste, abuse, and mismanagement to the OIG. In addition to receiving telephone calls at a toll-free Hotline number, we also accept emails through the Hotline email system and an online referral form. Visit https://naraoig.oversight.gov/ for more information, or contact us:

By telephone
Washington, DC, Metro area: 301- 837-3000
Toll-free: 800-786-2551

By facsimile
301-837-3197

By online referral form
https://naraoig.oversight.gov/online-complaint-form

Contractor Self-Reporting Hotline
As required by the Federal Acquisition Regulation, a web-based form allows NARA contractors to notify the OIG, in writing, whenever the contractor has credible evidence a principal, employee, agent, or subcontractor of the contractor has committed a violation of the civil False Claims Act or a violation of federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations in connection with the award, performance, or closeout of a contract or any related subcontract. The form can be accessed through the OIG's home page or found directly at https://naraoig.oversight.gov/oig-contractor-reporting-form.