This is the accessible text file for Library of Congress Office of the Inspector General report number 2023-IT-101, Final Audit Report– Inventory Controls for End User Devices Audit released on July 19, 2024.

FOR PUBLIC RELEASE

Office of the Inspector General

Library of Congress

Memo

Date July 19, 2024

To Dr. Carla Hayden
Librarian of Congress

From Debbie Lehrich
Acting Inspector General

Subject Final Audit Report– Inventory Controls for End User Devices Audit, Report No. 2023-IT-101.

This transmits the final report of the Office of the Inspector General's (OIG) audit of the Library of Congress's (Library) inventory controls for end user devices.

Based on management's written response to the draft report, we consider all of the recommendations resolved. Your response to the draft report provided an action plan and timeline for the implementation of each recommendation, in accordance with Library of Congress Regulation 9-160, Rights and Responsibilities of Library Employees to the Inspector General, §6.A.

We appreciate the cooperation and courtesies extended by the Office of the Chief Information Officer and the Integrated Support Services Directorate.

cc Principal Deputy Librarian of Congress

Chief Information Officer

Deputy Chief Information Officer

Chief Operating Officer

Director, Integrated Support Services

General Counsel

Sikich

PERFORMANCE AUDIT OF INFORMATION TECHNOLOGY INVENTORY CONTROLS FOR END USER DEVICES

SUBMITTED TO THE
LIBRARY OF CONGRESS
OFFICE OF THE INSPECTOR GENERAL

PERFORMANCE AUDIT REPORT

JULY 15, 2025

TABLE OF CONTENT

Ms. Debbie Lehrich
Acting Inspector General
Office of Inspector General
U.S. Library of Congress

Dear Ms. Lehrich:

Sikich CPA LLC (Sikich) (Footnote 1) is pleased to submit the attached report detailing the results of our performance audit of the Library of Congress's (LOC or Library's) information technology (IT) inventory controls for end user devices to determine the accuracy of the Library's inventory, the validity of the procure-to-disposal process, and the effectiveness of controls in operation.

The Library Office of the Inspector General (OIG) engaged Sikich to conduct this performance audit pursuant to Contract Number LCOIG22D0001, Task Order OIG23T0004.

Sikich conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Sikich performed the work from July 2023 through March 2024.

We thank the Library for the cooperation and assistance provided to us.

Sikich CPA LLC
Alexandria, VA
July 15, 2024

Footnote 1 - Effective December 14, 2023, we amended our legal name from "Cotton & Company Assurance and Advisory, LLC" to "Sikich CPA LLC" (herein referred to as "Sikich"). Effective January 1, 2024, we acquired CliftonLarsonAllen LLP (CLA's) federal practice, including its work for the Library of Congress.

I. EXECUTIVE SUMMARY

The Library OIG engaged Sikich to conduct a performance audit of the Library's IT inventory controls for end user devices (Footnote 2) to determine the accuracy of the Library's inventory, the validity of the procure-to-disposal process, and the effectiveness of controls in operation.

The Library is the largest library in the world and serves as the main research arm of the U.S. Congress. It has approximately 3,400 employees and additional contractor staff requiring IT assets (i.e., end user devices) to perform their work. Changing staff levels and warranty expiration dates affect the acquisition and replacement of technology assets.

In carrying out the audit objective, we assessed inventory controls for end user devices to determine if:

- The Library has documented and implemented procurement, receiving, storage, inventory, distribution, and disposal policies, procedures, and processes (i.e., the life cycle).
- The Library's controls over these inventories are consistent with National Institute of Standards and Technology (NIST) guidance.
- Controls have been implemented throughout the supply chain life cycle of end user devices to detect fraud or waste, including protecting the Library from unnecessary purchases and aging IT inventory.
- The Library's use of networked multi-function printers/scanners, licenses, and maintenance contracts is optimal and cost-efficient, given the Library's recent shift to more hybrid work location authorizations.
- The Library has restricted network (information system) access only to approved devices.

We performed our work through inquiries, observations, evaluation of relevant controls, and inspection of policies and procedures.

Key Library service units involved in the life cycle management of end user devices include the Library Office of the Chief Information Officer (OCIO) and Chief Operating Officer (COO). OCIO is responsible for managing the procurement, delivery, and retirement of end user devices.

The Integrated Support Services (ISS) directorate is part of COO and is responsible for the receipt, inspection, and assignment of unique identifying numbers to accountable property (i.e., personal property owned by the Library that is serialized and non-expendable); maintaining an automated accountable property sub-ledger Asset Management Tracking System (AMTS); providing the

Financial Services Directorate (FSD) with the information necessary to verify procurements; and disposal of capitalized property. OCIO is responsible for performing regular physical inventories to confirm the presence and location of end user devices.

We noted that the Library OIG has previously reported weaknesses in the Library’s controls related to end user devices. In July 2022, the Library OIG issued a report (Footnote 3) evaluating selected cybersecurity controls that identified weaknesses related to the inventory of hardware and system assets. Specifically, recommendation 2.1 noted that the Library needs to “develop formal procedures for maintaining an up-to-date inventory of hardware assets and removing unauthorized or unmanaged hardware assets in a timely manner.” Also, recommendation 2.3 noted that the Library needs to “maintain a complete, accurate, and centralized repository of all hardware assets connected to the LOC network.” Both recommendations remained open at the time of this audit.

Footnote 2 - For the purposes of this audit, end user devices refers to laptops, desktops, and multi-function devices (printers/scanners that have memory and connect to the network).

Footnote 3 - Fiscal Year 2021 Cybersecurity Controls Maturity Evaluation, Report No. 2021-IT-101 (July 13, 2022).

In June 2023, the Library OIG issued a report (Footnote 4) identifying weaknesses related to the inventory of hardware and system assets. Specifically, recommendation 3.1—which notes that the Library needs to “acquire and implement an automated solution to ensure the timely, consistent, and accurate inventory and mapping of system assets.” This recommendation remained open at the time of this audit.

We found that management has initiatives in process as part of the Library’s efforts to improve the accuracy of its end user device inventory, the validity of its procure-to-disposal process, and the effectiveness of its controls in operation. For example, the Library is in the process of approving a Library of Congress Regulation (LCR) related to IT asset management. In addition, the Library is developing an automated asset management solution with an expected deployment in the first quarter of fiscal year 2025, with related procedures and workflows to follow.

However, until the Library has implemented these initiatives, weaknesses remain in the Library’s controls over the timeliness, completeness, accuracy, documentation, and handling of its end user device inventory process. We concluded that, although the Library has documented and communicated controls over the operation of its end user devices, there were inconsistencies in the implementation of the controls. Specifically, in addition to the noted prior year audit issues discussed previously, we noted the following areas of improvement necessary to strengthen the Library’s inventory controls for end user devices.

1. The Library’s inventory for end user devices does not accurately reflect its current information system.

The Library has not been conducting annual physical inventories of end user devices, including laptops and multi-function devices (MFDs),(Footnote 5) in accordance with requirements in Library Directive (LCD) 5-410-1, Information Technology Security Program (ITSEC). OCIO completed its most recent inventory in December 2019 and was in the process of conducting such an inventory at the time of our audit. In addition, the Library does not include leased MFDs in its physical inventory.

2. The Library’s IT asset records are not current and complete.

We found discrepancies between information that ISS logistics personnel input into AMTS (Footnote 6) and information that OCIO obtained via annual physical inventories, as well as instances in which AMTS records were not current. For example, we identified: end user devices that connected to the network but that were not listed in AMTS or were marked as retired in AMTS; end user devices that were marked as retired in AMTS but were missing retirement dates; end user devices that we observed at the Library but that were not listed in AMTS; end user devices that OCIO included in its inventory but that were not listed in AMTS; and incorrect purchase order numbers in AMTS.

Footnote 4 - Fiscal Year 2022 CRS IT Modernization Performance Report, Report No.2022-IT-103.

Footnote 5 - For the purposes of our audit, MFDs are devices that have memory and operating software and that connect to the Library’s internal network.

Footnote 6 - Library logistics personnel use AMTS to track non-capitalized equipment (i.e., equipment valued at less than $50,000), including end user devices, from receipt to final disposition.

3. The Library has inadequate controls over the tracking of digital media devices through sanitization and destruction prior to final disposition.

We found that actual responsibilities for sanitization processes were not in accordance with stated policies. Although OCIO stated that they sanitized digital media devices (e.g., external/removable hard disk drives, flash drives) prior to releasing them to the ISS Automation Team, LCD 8-330.1, Cleaning Hard Drives of Surplus Computers, requires the Automation Team to perform the sanitization procedures. In addition, OCIO could not provide documentation showing that it had sanitized digital media devices before the Automation Team processed the devices for final disposition for the 6 months under review.

4. The Library stopped requiring property passes for Library Government Furnished Equipment (GFE) but has not updated its related policies and procedures.

The Library has not updated its regulations to reflect current processes and practices related to property passes. Specifically, despite current Library regulation (Footnote 7) requirements, the Library stopped requiring property passes for laptops and government mobile devices, and the Library’s ISS Logistics Services asset control team has not maintained a current and complete list of individuals authorized to issue and sign property passes. Additionally, the Library has not updated this regulation to reflect that ISS and the Library’s Security & Emergency Preparedness Division are implementing an automated system to collect and publish authorized signatories of property passes and clarify how the Library will use this data to protect Library GFE.

II. BACKGROUND

The Library is the world’s largest library, with more than 175 million items in its collections and extensive expert services and programs. It is the main research arm of the U.S. Congress and has six primary service units:

- Office of the Librarian
  - Strategic Planning and Performance Management
- Office of the Chief Operating Officer
  - Integrated Support Services
- Office of the Chief Information Officer

- Library Collections & Services Group, which includes:
  - Law Library
  - National Library Service
  - Research and Collection Services
  - Discovery and Preservation Services

- U.S. Copyright Office (USCO)

- Congressional Research Service

Footnote 7 - LCR 8-320, Asset Control of Equipment and Furniture (dated September 2008).

These service units are organized as follows:

IMAGE: ORGANIZATION CHART

AS OF JULY 3, 2023

Top level: Carla Hayden, Librarian of Congress. Reporting to Hayden: Mark Sweeney, Deputy Librarian of Congress.

Six primary Library components report to the Librarian and Deputy Librarian of Congress:

Library Collections and Services Group (LCSG),

Office of the Chief Information Officer (OCIO),

Office of the Chief Operating Officer (COO),

Congressional Research Service, U.S. Copyright Office (USCO), and

the Office of the Librarian

There a two independent Offices at the Library of Congress: the Office of the Inspector General (Footnote 1) and Copyright Royalty Board (Footnote 2).

1. Office of the Librarian is made up of the Center for Exhibits and Interpretation, Center for Learning, Literacy and Engagement, Office of the General Counsel (Footnote 3) and Strategic Planning and Performance Management. Also within the Office of the Librarian is the Office of the Chief of Staff, Ryan Ramsey, Chief of Staff and the Office of Communications and external Relations, Roswell Encina, Chief Communications Officer. Four units report to Ryan Ramsey: Congressional Relations Office; Development Office; EEO and Diversity Programs; and Office of the Librarian and Centers Administration. Two units report to Roswell Encina: Communications and the Multimedia Group.

2. LCSG: Robin L. Dale, Deputy Librarian for LCSG with five service units reporting to Robin Dale:

LCSG Operations, made up of Financial Management and Organizational Management:

National Library Service for the Blind and Print Disabled, Jason Broughton, Director;

Law Library, Aslihan Bulut, Law Librarian with three divisions reporting to Aslihan Bulut: Office of External Relations, Global Legal Collections, and Global Legal Research;
Research & Collections Services, Hannah Sommers, Associate Librarian for Researcher and Collections Services with four divisions reporting to Hannah Sommers: Collection Development Office, National Audio-Visual Conservation, John W. Kluge; Center, General & International Collections, and Special Collections;
Discovery & Preservation Services, Katherine R. Zwaard, Associate Librarian for Discovery and Preservation Services with three units reporting to Katherine R. Zwaard: Acquisitions & Bibliographic Access, Digital Services, Preservation.

3. OCIO, Judith Conklin, Chief Information Officer with seven service units reporting to Judith Conklin: Digital Strategy; IT Governance; IT Financial Management; IT Quality & Performance Management; IT Design and Development; IT Partner Engagement; IT Service Operations.

4. COO, Edward R. Jablonski, Chief Operating Officer with units reporting to Edward Jablonski: Chief Financial Officer/Financial Service; Contracts and Grants; Human Capital; Integrated Support Services; Library Enterprises; Security and Emergency Preparedness.

5. CRS, Robert R. Newlen, Interim Director with eleven units reporting to Robert Newlen: Deputy Director; Administrative Operations; Office of Legislative Information; Office of Publishing; Counselor to the Director; American Law; Domestic Social Policy; Foreign Affairs, Defense and Trade; Government and Finance; Knowledge Services Group; Resources, Science and Industry.

6. USCO, Shira Perimutter, Register of Copyrights and Director with six units reporting to Shirma Perimutter: General Counsel; Policy and International Affairs; Registration Policy and Practice; Public Information and Education; Operations; Copyright Records.

Footnote 1 of organization chart - The Library of Congress Inspector General Act of 2006 (PL 109-66), effective August 2, 2005, requires that the Inspector General shall report to, and be under the general supervision of the Library of Congress.

Footnote 2 of organization chart - The Copyright Royalty and Distribution Act of 2004 (PL 108-419), effective May 31, 2005, replaced the Copyright Arbitration Royalty Panel System with the Copyright Royalty Judges, who are appointed by the Librarian of Congress.

Footnote 3 of organization chart - The General Counsel serves as counsel to the Executive Committee.

Figure A: Library of Congress Organization Chart (Footnote 8)

Office of the Chief Information Officer: The Library's OCIO is responsible for managing the procurement, delivery, and retirement of end user devices. It is also responsible for overseeing the Library's IT investments, including reviewing and approving IT procurements such as printers and document-scanning equipment (network and desktop), laptops, desktop workstations, monitors and tablets, software licenses and maintenance, and all IT services, including cloud services and developing, implementing, performing regular physical inventories, and enforcing Library IT policies and procedures.

Integrated Systems Support: The Library’s ISS directorate is part of the COO service unit and is responsible for the receipt, inspection, and assignment of unique identifying numbers to accountable property (i.e., personal property owned by the Library that is serialized and non-expendable); maintaining an automated accountable property sub-ledger, AMTS; providing FSD with the information necessary to verify the procurement and disposal of capitalized property; and performing regular physical inventories and advising FSD of updates to reflect the results of the inventories.

Footnote 8 - https://loc.gov/static/portals/about/documents/current-library-org-chart.pdf

III. AUDIT RESULTS

We identified the following findings during our audit.

Finding 1: The Library’s inventory for end user devices did not accurately reflect its current information system.

Background

Upon receiving end user devices from vendors, the ISS Logistics Services Division (ISS/LOG) verifies and stores the devices at the warehouse and sends copies of packing lists to relevant contracting officer’s representatives in the OCIO to inform them that their devices have arrived. ISS/LOG activities include scanning barcodes on the devices to record them in the AMTS. Upon request from OCIO, ISS/LOG ships the devices to OCIO for configuration and deployment to end users. OCIO is then responsible for user maintenance and the accounting of these devices in their custody. OCIO performs an annual physical inventory of end user devices to confirm what is in their possession and relies on AMTS records for inventory tracking purposes along with the information OCIO obtains via its annual physical inventories.

OCIO stated that when end user devices are ready for disposal, they remove and destroy the hard drives, then pack the devices on a palette and submits a surplus request to ISS. At this point, they are no longer considered connected to the network. ISS updates AMTS and a separate spreadsheet to reflect that the devices were received from OCIO and cleared of data. These procedures are described in detail in LCD 8-330.1, Cleaning Hard Drives of Surplus Computers.

Condition

The last physical inventory of the Library end user devices, including MFDs, had not been conducted since December 2019. The Library was in the process of conducting such an inventory at the time of this audit. Further, the Library stated that it does not treat leased MFDs as being part of its inventory.

Criteria

LCR 8-320, Asset Control of Equipment and Furniture, (dated September 2008), states the following responsibilities regarding the use, maintenance and accounting of accountable property (encompasses end user devices) and asset control:

3.A.1

The Executive Committee will determine which accountable property that is not capitalized property, such as weapons, information technology equipment, and electronic communications equipment, should be subject to asset control and included in the AMTS.

3.A.4.

Service units are each responsible for the proper use, maintenance and accounting of all accountable property2F in their custody. To fulfill this responsibility, each service unit shall appoint a knowledgeable staff member as a property liaison to maintain effective control of all accountable property (Footnote 9) in the service unit. The number of property liaisons shall be commensurate with the volume and geographic dispersion of accountable property in the service unit. Property liaisons shall maintain proper control over all accountable property assigned to their service units by working directly with the ISS/(LOG) property management officer to establish and maintain positive accountability of accountable property in the custody of the service throughout the life-cycle of each asset (from acquisition to disposal). Additionally, each property liaison shall ensure the service unit’s compliance with the annual inventory plan.

LCD 5-410.1, ITSEC (dated June 2023), states the following with regard to security control CM-8, System Component Inventory:

3.1.a

Every LC computing resource is identified as an information system or as a part of an information system (Major Application or General Support System). This identification must include a defined system inventory of all IT system components within the authorization boundary, appropriate to the granularity deemed necessary for tracking and reporting.

3.1.x

The LC IT Security Program must conduct an annual review of the Library's IT system inventory in line with the LOC's Inventory Management Program.

4.8.a

All information systems and networks are appropriately documented in such a way as to allow others to understand system operation and configuration.

4.9.d

OCIO shall ensure that each network printer, copier, and facsimile machine is within the system definition of a LC information system that has a current ATO.

LCR 5-410, IT Security Policy, (dated November 2015) states the following regarding responsibilities:

F. Service units are responsible for:

1. Ensuring implementation of, and compliance with, the IT security plan within the unit

2. Ensuring best security practices are implemented and maintained throughout the system life cycle of each IT system under their control.

Footnote 9 - Per LCR 8-320, Asset Control of Equipment and Furniture, September 2008, the term "accountable property" is defined as meaning both (1) facility leasehold improvements, and (2) personal property owned by the Library that is serialized and non-expendable (that has a continuing use as a self-contained unit, is not consumed when put to use, does not lose its identity when put to use, and does not ordinarily become a component of other equipment). “Accountable property” also includes real and personal property obtained using a capital lease.

The Library’s System Security Plan for the Library of Congress Imaging Services MFD (dated March 2023) states that the Library has allocated the following security controls to the system:

CM-08: The ISSO [Information System Security Owner] ensures that an IT system inventory is maintained for all hardware components (if applicable) and software licenses associated with Imaging Services System, including manufacturers, model numbers, serial numbers, and license numbers.

Cause

The Library’s current process for OCIO to receive, deploy, and retire end user devices relies upon multiple tracking systems (e.g., AMTS, PCBoot (Footnote 10) reports, and PC cleaning database) and an annual physical inventory process.

Additionally, the Library’s annual physical inventory process was not performed timely.

Effect

Without an inventory of end user devices that includes all MFDs, the Library cannot adequately assure protection from unauthorized, unanticipated, or unintentional access, disclosure, or modification of assets required for agency operations.

Without regular verification of the existence of equipment, there is an increased risk of misuse or misappropriation of this equipment,(Footnote 11) unnecessary purchases, and aging IT inventory, as previously reported in the audit of the Library’s ISS: Improvements Needed to Prevent Wasteful Procurement and Inefficient Disposal of IT Workstations (Audit Report No. 2012-PA-101, September 2012).

Recommendation

We recommend that the Library:

1.1 Complete the inventory of Library end user devices being conducted at the time of this audit, to include all MFDs, including those that are leased.

Finding 2: The Library's IT asset records were not current and complete.

Background

Although not required to do so by Library policy, Library logistics personnel use AMTS (Footnote 12) to track non-capitalized equipment (i.e., equipment valued at less than $50,000), including end user devices, from receipt to final disposition. Upon receiving the devices from vendors, logistics personnel located in Logistics Services in the ISS Directorate verifies the contents and sends copies of packing lists to relevant contracting officer's representatives (CORs) in OCIO. The CORs then mark the items as received on the original purchase orders and authorize payment for the devices. The logistics personnel also scan barcodes on the devices to record them in AMTS. OCIO relies on AMTS records for inventory tracking purposes, along with the information OCIO obtains via its annual physical inventories. Library IT Security Directive 5-410.1 states that an annual review of the Library's IT system inventory must occur as part of the IT Security Program, in line with the Inventory Management Program.

Footnote 10 - A listing of devices which had connected to the LOC network over the previous 30 days from when the report was generated.

Footnote 11 - The U.S. Department of Justice announced on January 4, 2023, that, pursuant to an investigation initiated by the Library OIG, an individual was sentenced to one year of probation, to include six months of home confinement, for stealing government property from the Library and the Department of Commerce from on or about 2017 until 2020. The individual worked as a contractor providing IT support services at the Library in Washington, D.C. While at the Library, the individual removed at least 29 separate Dell laptops that he knew belonged to the Library (cumulatively worth a total of approximately $55,590), advertised them on eBay, and ultimately resold them to different customers through that account.

Footnote 12 - AMTS is a module within the IBM TRIRIGA application suite.

For the purposes of our audit, MFDs are devices that have memory and operating software and connect to the Library's internal network. MFDs can also scan, print, and copy documents. Users are required to log in with their Library credentials to use MFDs, which assists in tracking usage and verifying that the person using the device is an authorized user.

Condition

We identified discrepancies between information that logistic personnel input into AMTS and information that OCIO obtained via its annual physical inventories, as well as instances in which AMTS records were not current. These discrepancies included the following examples:

- The Library had not updated AMTS to include 8 desktops and laptops that were connected to the Library network but were not listed in AMTS within 30 days of our fieldwork period, based on our comparison of a listing of 4,845 laptops and desktops that the Library had recently connected to a listing of 12,668 devices identified in AMTS (excluding draft or retired assets).

- One hundred end user devices marked as retired in a December 2023 AMTS inventory listing were still connecting to the network in December 2023. In addition, AMTS did not include a retirement date for any of the 100 devices.
- We noted that 59 percent of all the devices listed in AMTS as retired (42,789 of 72,481) were missing retired dates.
- OCIO's inventory list included 68 laptops and desktops which were unable to be reconciled to AMTS by their serial number or barcode.
- The Library did not include 5 of the 12 desktops and printers observed as in-use during a physical onsite inspection conducted on November 13, 2023, in an AMTS inventory listing dated November 8, 2023.
- The Library had incorrectly documented 225 of the 400 desktops listed on a recent purchase order (i.e., the Library input the incorrect purchase order numbers in AMTS). ISS subsequently informed the auditors that the Library had addressed these discrepancies.
- The Library did not include any MFDs in either AMTS or OCIO's physical inventory data.

Criteria

NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations (dated December 2020), states the following regarding system component inventory controls:

- Determine if the organization: CM-8(a) CM-8(a)(1) develops and documents an inventory of information system components that accurately reflects the current information system;

a. Develop and document an inventory of system components that:

1. Accurately reflects the system;
2. Includes all components within the system;

3. Does not include duplicate accounting of components or components assigned to any other system;

4. Is at the level of granularity deemed necessary for tracking and reporting; and

5. Includes the following information to achieve system component accountability: [Assignment: organization-defined information deemed necessary to achieve effective system component accountability]; and

b. Review and update the system component inventory [Assignment: organization-defined frequency].

The Library's Information Technology Security Directive 5-410.1 (dated June 2023) states the following with regard to security control CM-8, System Component Inventory:

Policy ID 3.1.a

Every LC computing resource is identified as an information system or as a part of an information system (Major Application or General Support System). This identification must include a defined system inventory of all IT system components within the authorization boundary, appropriate to the granularity deemed necessary for tracking and reporting.

Policy ID 4.8.a

All information systems and networks are appropriately documented in such a way as to allow others to understand system operation and configuration.

Cause

The Library did not reconcile information that its logistic personnel input into AMTS to the information that OCIO obtained via its annual physical inventories in a timely manner to ensure that the Library's inventory of physical IT devices was current and accurate. OCIO stated that an automated IT asset management solution was under development and that it was expected to reduce the risk of discrepancies attributable to having the two different sources of inventory information. The system is scheduled for completion in the first quarter of FY 2025.

Further, the Library did not have documented, formal procedures in place for reconciling the two sources of inventory information. An IT asset management system solution was under review at the time of our fieldwork. Documented procedures are necessary to facilitate management review and approval and to ensure consistent performance in areas such as end user devices.

Effect

Without current and complete asset records for end user devices and adequate oversight of related internal controls for such equipment, there is an increased risk of Library service units not being able to accurately account for the end user devices under their authority. This increases the likelihood of theft, misuse, or misappropriation of the devices, in addition to potentially increasing the likelihood of wasteful purchases of such equipment. Further, the lack of current and complete asset records for end user devices could delay efforts to discover and recover missing devices.

Recommendations

We recommend that the Library:

2.1 Complete OCIO’s development and implementation of an automated IT asset management solution.

2.2 Finalize the development of formal procedures for maintaining an up-to-date inventory of hardware assets, from acquisition to final disposition, including all end user devices and MFDs, as well as such devices purchased without the involvement of Library logistics personnel. (Footnote 13)

Finding 3: The Library has inadequate controls over the tracking of digital media devices through sanitization and destruction prior to final disposition.

Background

Library personnel use digital media devices that electronically store data of varying levels of security classifications. The Library must appropriately manage these devices at the end of their useful lives by using NIST compliant sanitization and destruction methods. The applicable method depends on the classification of the data on the device. The purpose of these activities is to prevent unauthorized disclosure of information.

Condition

OCIO stated that it sanitized digital media devices prior to releasing them to the Automation Team in the ISS Directorate. However, LCD 8-330.1, Cleaning Hard Drives of Surplus Computers, requires the Automation Team to perform this function.

In addition, OCIO could not provide documentation showing that it had sanitized digital media devices before the Automation Team processed the devices for final disposition for the 6 months under review (i.e., October and December of 2022 and February, April, June, and July of 2023).

Criteria

LCD 8-330.1, Cleaning Hard Drives of Surplus Computers (dated March 2008), states the following with regard to responsibilities for hard drive sanitization:

- Section 4. Procedures, Sub section 4.3

Hard Drive Cleansing of Computers by ISS Automation Team – The automation team cleanses the Central Processing Unit (CPU) on each computer using the Disk Eraser application (via CD-ROM). Six (6) passes and one (1) verify are performed on each CPU. The verify process ensures that all data has been removed from the CPU. The ISS Automation team staff records on a tag the barcode number and CPU serial number for each cleansed computer and affixes the tag to the cleaned unit. Each barcode number is recorded onto a checklist which is given to the Logistics' receiving team member when the cleaned computers are collected.

Footnote 13 - The Library previously agreed to a recommendation to maintain an up-to-date inventory of hardware assets that did not specifically include end user physical IT devices. As stated in OIG Audit Report No. 2021-IT-101, Cybersecurity Controls Maturity Report, recommendation 2.1: "Develop formal procedures for maintaining an up-to-date inventory of hardware assets and removing unauthorized or unmanaged hardware assets in a timely manner."

LCD 5-410.1, ITSEC (dated June 2023), states the following with regard to security control MP-6, Media Sanitization:

Policy ID 4.3.3.a

Media containing information categorized as Moderate or Low must be sanitized or destroyed per NIST Special Publication (SP) 800-88, Firmware purge commands (if available on the drive) or using the Secure Erase function (if available on the drive) before disposal or release to another organization for reuse.

Policy ID 4.3.3.c

Media containing information categorized as High must be destroyed per NIST SP 800-88 before disposal.

Policy ID 4.3.3.d

Audit logs must be kept concerning all media disposal, destruction, and sanitization actions, including date of action, personnel performing action, and item/data description of item being disposed of, destroyed, or sanitized.

NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations (dated December 2020), indicates the following with regard to media sanitization controls:

- MP-6 Media Sanitization

Control

a. Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; and

b. Employ sanitization mechanisms with strength and integrity commensurate with the security category or classification of the information.

NIST SP 800-88, Revision 1, Guidelines for Media Sanitization (dated December 2014), states the following regarding the safeguarding of electronic media:

In order for organizations to have appropriate controls on the information they are responsible for safeguarding, they must properly safeguard used media. An often-rich source of illicit information collection is either through dumpster diving for improperly disposed hard copy media, acquisition of improperly sanitized electronic media, or through keyboard and laboratory reconstruction of media sanitized in a manner not commensurate with the confidentiality of its information.

Cause

The Library lacks a current, formal process for documenting the OCIO and ISS responsibilities, procedures, and recordkeeping controls necessary to effectively track digital media devices through sanitization and destruction prior to their final disposition, as required by LCD 5-410.1 Information Technology Security Directive, June 2023, Policy ID 4.3.3d.

Effect

Under current practices, the Library is not assured that all data on its digital media devices are appropriately removed prior to the device’s final disposition. This could lead to sensitive information being moved from a secure environment to an unsecured one, making the information accessible to outsiders or unauthorized individuals.

Recommendations

We recommend that the Library:

3.1 Update LCD 8-330.1 to assign responsibility for the sanitization and destruction of digital media devices.

3.2 Develop a formal process to document the OCIO and ISS responsibilities, procedures, and recordkeeping controls necessary to effectively track digital media devices through sanitization and destruction prior to the devices' final disposition.

Finding 4: The Library stopped requiring property passes for Library GFE but did not update its related policies and procedures.

Condition

The Library has not updated LCR 8-320, Asset Control of Equipment and Furniture, to reflect that the Library stopped requiring property passes for laptops and government mobile devices and that the Library's Logistics Services asset control team located in the ISS Directorate is not maintaining a current and complete list of individuals authorized to issue and sign property passes. Additionally, the regulation has not been updated as appropriate to reflect that ISS and the Library's Security & Emergency Preparedness Division are implementing an automated system to collect and publish authorized signatories of property passes and how this data would be utilized to protect the Library's GFE. The Library indicated that it is working to update the regulation.

Criteria

LCR 8-320, Asset Control of Equipment and Furniture (dated September 2008), states the following:

5. Property Passes

The ISS Logistics asset control unit shall maintain and manage LOC’s property pass authorization list that designates individuals who are authorized to sign a government property pass to remove accountable property from LOC. The asset control unit will provide the list to U.S. Capitol Police and maintain a current list on the ISS intranet website to allow for the verification of signatures displayed on passes when employees exit LOC buildings with LOC property and for offices to periodically verify and validate the personnel listed as authorized signatories.

Cause

Library management decided to stop requiring property passes for laptops and government mobile devices exiting Library facilities, without updating the associated LCR.

Effect

When the Library stopped requiring property passes for laptops and government mobile devices and therefore also stopped maintaining a list of individuals authorized to issue and sign property passes, LCR 8-320 became out of date. This undermines the Library’s capability to enforce its new practices and ensure that it protects its GFE, increasing the risk that the Library may lose IT assets containing Library data.

Recommendation

We recommend that the Library:

4.1 Revise LCR 8-320, as well as other regulations and directives as appropriate, to accurately reflect the Library’s desired operational control environment related to laptop and government mobile device physical security and the use of property passes.

APPENDIX A – OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this performance audit was to assess the effectiveness of the Library's IT inventory controls for end user devices and determine the accuracy of the Library's inventory, the validity of the procure-to-disposal process, and the effectiveness of controls in operation. In carrying out this objective, we assessed controls relevant to end user devices to determine if:

- The Library has documented and implemented procurement, receiving, storage, inventory, distribution, and disposal policies, procedures, and processes (i.e., the life cycle).
- The Library's controls over these inventories are consistent with NIST guidance.
- Controls have been implemented throughout the supply chain life cycle of end user devices to detect fraud or waste, including protecting the Library from unnecessary purchases and aging IT inventory.
- The Library's use of networked multi-function printers/scanners, licenses, and maintenance contracts is optimal and cost-efficient, given the Library's recent shift to more hybrid work location authorizations.
- The Library has restricted network (information system) access only to approved devices.

We performed our work through inquiries, observations, evaluation of relevant controls, and inspection of policies and procedures.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We conducted this audit from July 2023 through March 2024.

Our procedures included the following steps to satisfy our audit objectives:

- Inquiring with the IT Chief, Director of IT Financial Management, End User Services Division Chief, Supervisory Inventory Specialist, Chief of Logistics, Logistics Manager, and other relevant Library personnel regarding the procurement of IT equipment to determine how the Library received, stored, inventoried, and distributed the equipment.
- Inspecting Library directives, policies, and procedures, including but not limited to:
    - The Library of Congress Information Technology Security Directive 5-410.1, General Information Technology Security (June 2023)
    - LCD 6-310.1, Accounting for Capitalized Property and Depreciation (December 2015)
    - LCD 8-330.1, Cleaning Hard Drives of Surplus Computers (March 2008)
    - LCR 8-320, Asset Control of Equipment and Furniture (September

- Inspecting other documents, reports, and evidence provided by the Library, including:
    - Purchase orders
    - Asset inventories
    - Contracts
    - MFD usage reports
    - End user device sanitization and disposal records
    - Licensing and maintenance agreements

- Evaluating a sample of networked multi-function printers and scanners and obtaining usage reports over time for the device. Assessing usage metrics to determine whether devices were currently in use and, if the device was seeing lower use, inquiring with management whether the device was still required.

- Inspecting a sample of IT equipment from the current inventory to determine whether the Library had accurately identified and authenticated the device through its approved processes.

- Inspecting a sample of unidentified or unauthorized devices in the inventory to determine the current location or disposition of the asset.

We assessed internal controls that we deemed to be significant to the audit objective. Specifically, we assessed 3 of the 17 principles associated with the five components of internal control defined in the Government Accountability Office’s (GAO’s) Standards for Internal Controls for the Federal Government (September 2014) (Green Book). The table below summarizes the principles we assessed:

Table 1: GAO Green Book Assessment Principles

Risk Assessment
Principle 8: Potential for fraud when identifying, analyzing, and responding to risks.
Control Activities
Principle 10: Design Control Activities
Principle 11: Design Activities for the Information System

Through our assessment of internal controls, we identified deficiencies that could affect the design, implementation, and operating effectiveness of these internal controls and that we believe could affect the Library; we have included the results in this report.

APPENDIX B – MANAGEMENT COMMENTS

We provided Library management with our draft version of this report, and Library management provided the following responses. We have not evaluated management's responses and therefore do not express an opinion on them.

MEMORANDUM

Date July 8, 2024
To Debbie Lehrich, Acting Inspector General
From J. Mark Sweeney, Principal Deputy Librarian of Congress
Subject Management Response to OIG report 2023-IT-101, Performance Audit of Information Technology Inventory Controls for End User Devices

The Library of Congress generally concurs with the recommendations in the Office of the Inspector General (OIG) report on the information technology inventory controls for end user devices.

The Office of the Chief Information Officer (OCIO) is already in the process of developing an automated IT asset management (ITAM) solution. Moreover, the draft ITAM policy, which is currently under review by Library service units: assigns responsibilities for IT assets from acquisition and delivery through disposition; addresses maintenance of a centralized IT asset repository; and seeks to align ITAM data with existing asset management tracking tools used by the Integrated Support Services

Directorate (ISS). Finally, OCIO and ISS are collaborating to ensure the Library's policies accurately, succinctly, and comprehensively address asset control to improve compliance and to maintain security of Library information.

The attached chart provides additional details on the Library's corrective action plans and target completion dates in response to the individual report recommendations.

cc: Judith Conklin, Chief Information Officer
Edward Jablonski, Chief Operating Officer
Meg Williams, General Counsel

Management Comments on Draft OIG Report No. 2023-IT-101, Inventory Controls for End User Devices

Recommendation # 1.1 Complete the inventory of Library end user devices being conducted at the time of this audit, to include all MFDs, including those that are leased. Responsible Office OCIO - The Library will complete the inventory of Library end user devices being conducted at the time of this audit, to include all MFDs, including those are leased. Target completion FY25 Q2.

Recommendation # 2.1 Complete OCIO's development and implementation of an automated IT asset management solution. Responsible Office OCIO in conjunction with ISS - The Library will complete OCIO's development and implementation of an automated IT asset management solution. Target completion FY25 Q4.

Recommendation # 2.2 Finalize the development of formal procedures maintaining an up-to-date inventory of hardware assets, from acquisition to final disposition, including all end user devices and MFDs, as well as such devices purchased without the involvement of Library logistics personnel. Responsible Office OCIO in conjunction with ISS - Finalize the development of formal procedures maintaining an up-to-date inventory of hardware assets, from acquisition to final disposition, including all end user devices and MFDs, as well as such devices purchased without the involvement of Library logistics personnel. Target Completion FY25 Q4.

Recommendation # 3.1 Update LCD 8-320.1 to assign responsibility for the sanitization and destruction of digital media devices. Responsible Office OCIO (in conjunction with ISS) - OCIO will update LCD 8-330.1 to assign responsibility for the sanitization and destruction of digital media devices. Target Completion FY25 Q1.

Recommendation # 3.2 Develop a formal process to document the OCIO and ISS responsibilities, procedures, and recordkeeping controls necessary to effectively track digital media devices through sanitization and destruction prior to the devices' final disposition. Responsible Office OCIO in conjunction with ISS - The Library will develop a formal process to document the OCIO and ISS responsibilities, procedures, and recordkeeping controls necessary to effectively track digital media devices through sanitization and destruction prior to the devices' final disposition. Target Completion FY25 Q1.

Recommendation # 4.1 Revise LCR 8-320, as well as other regulations and directives as appropriate, to accurately reflect the Library's desired operational control environment related to laptop and government mobile device physical security and the use of property passes. Responsible Office ISS - The Library will revise LCR 8-320 to align with related regulations and directives and to accurately reflect the Library's desired operational control environment and related to laptop and government mobile device physical security and the use of property passes. This revision will incorporate current practices being implemented at the Library. ISS anticipates a draft of the revised regulation around July 31, 2024. By revising LCR 8-320 and related regulations to accurately reflect the Library's operational control environment for laptop and government mobile device security, as well as property pass management, the Library will enhance its security measures, improve compliance, and optimize operational efficiency in asset management and security practices. Target Completion FY25 Q3.