

Office of Inspector General
U.S. Government Accountability Office

Information Technology Assets

Risk Assessments Could Inform Inventory
Activities during Future Disruptions

Accessible Version



**Office of Inspector General
U.S. Government Accountability Office
Report Highlights**

June 8, 2023

INFORMATION TECHNOLOGY ASSETS

Risk Assessment Actions Could Inform Inventory Activities during Future Disruptions

Objective

GAO shifted to a remote operating posture to help protect employees during the COVID-19 pandemic. This posed challenges for GAO's annual inventory of accountable property—which includes Information Technology (IT) assets like laptops, hard drives, scanners, mobile storage devices, and printers. These assets may process and potentially store information under GAO's authority or control that requires protection from unauthorized disclosure, including classified information. Given the potential for national security, privacy, and other major risks as well as reputational, mission, and fraud risks if these items are lost, stolen, or otherwise missing, OIG examined Infrastructure Operation's (IO) inventory control over certain IT assets during the onset and height of the pandemic.

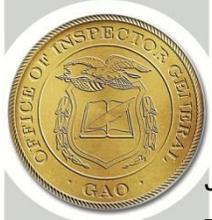
What OIG Found

GAO's IO office cancelled all fiscal year 2020 inventory activities, including for 3,579 IT assets that were inventoried in 2019. IO did not leverage existing inventory procedures that verify barcodes and locations through email correspondence to account for IT assets assigned to specific individuals within GAO. In addition, IO did not consider the impact of cancelling inventory, a principal antifraud control activity, on the IT asset fraud risks identified or revise the IT asset fraud risk profile accordingly.

In fiscal year 2021, IO inventoried a sample of GAO's accountable personal property that included less than 20 percent (1,035) of the 5,374 IT assets OIG reviewed that may process and store sensitive information. While the majority (162) of the IT assets designated as classified IT equipment were inventoried, just over 15 percent (41) did not have an inventory date. IO officials said they developed a risk-based inventory plan to restart activities at GAO headquarters but were unable to provide documentation of any risk assessment performed for the purpose of sample selection. Such an assessment should have indicated the most significant property risks IO identified and assessed; the magnitude of those risks; alternatives to GAO's annual inventory activities that IO had evaluated to address those risks; and rationales for including property such as cafeteria, fitness center, and mailroom equipment in the modified inventory, but excluding most of the IT assets OIG reviewed.

What OIG Recommends

OIG recommends that GAO take two actions: (1) develop and document procedures to update or revise IT asset fraud risk profiles when unexpected or unanticipated events occur, such as operating posture disruptions or changes to GAO's telework program; and (2) develop and document procedures to ensure that the appropriate risk-based assessments are completed when planning to implement an alternative to GAO's full annual inventory to ensure samples are targeted to the highest-risk IT assets. GAO agreed with the recommendations.



June 8, 2023

To: Gene L. Dodaro
Comptroller General of the United States

From: L. Nancy Birnbaum
Inspector General

A handwritten signature in black ink, appearing to be "L. Nancy Birnbaum", is written over the "From:" line.

Subject: Transmittal of Office of Inspector General's (OIG) Audit Report for Agency Comment

Attached for your information is our report, *Information Technology Assets: Risk Assessment Actions Could Inform Inventory Activities during Future Disruptions* (OIG-23-1). The audit objective was to examine Infrastructure Operation's inventory control over certain IT assets during the onset and height of the pandemic.

The report contains two recommendations aimed at developing and documenting important risk assessments and considerations in response to changes such as unanticipated events and planned alternatives to GAO's full annual inventory. In its written comments, GAO concurred with the recommendations. Management comments are included in Appendix II of our report. Actions taken in response to our recommendations are expected to be reported to our office within 60 days.

We are sending copies of this report to the other members of GAO's Executive Committee, GAO's Congressional Oversight Committees, GAO's Audit Advisory Committee, and other GAO managers, as appropriate. The report is also available at <https://www.gao.gov/ig> and <https://www.oversight.gov/reports>.

If you have questions about this report, please contact me at (202) 512-9355 or BirnbaumL@gao.gov.

Attachment

cc: Orice Williams Brown, Chief Operating Officer
Karl Maschino, Chief Administrative Officer/Chief Financial Officer
Edda Emmanuelli-Perez, General Counsel
Lisa Binckes, Acting Managing Director, Infrastructure Operations
William Anderson, Controller/Deputy Chief Financial Officer
Adebiyi Adesina, Special Assistant to the Controller
Jennifer Ashley, Special Assistant for Operational Initiatives

Table of Contents

INFORMATION TECHNOLOGY ASSETS.....	i
Objective	i
What OIG Found	i
What OIG Recommends.....	i
Introduction	1
Objective, Scope, and Methodology	1
Background.....	2
Roles and Responsibilities for Annual Inventory of Accountable Property.....	2
Conclusions.....	12
Recommendations for Executive Action	12
Agency Comments	13
Appendix I: Objective, Scope, and Methodology.....	14
Appendix II: Comments from the U.S. Government Accountability Office	16
Accessible Text for Appendix II: Comments from the U.S. Government Accountability Office	19
Appendix III: OIG Contact and Staff Acknowledgments	21
Appendix IV: Report Distribution.....	22
U.S. Government Accountability Office.....	22
GAO Audit Advisory Committee.....	22

Tables

Table 1: Accountable Personal Property Classification, Acquisition Threshold, and Control . 2

Table 2: GAO Policy Governing Designations and Responsibilities for Accountable Personal Property..... 3

Table 3: Annual Inventories of IT Assets That May Process and Store Sensitive Information, as of September 2022 8

Accessible Data for Table 3: Annual Inventories of IT Assets That May Process and Store Sensitive Information, as of September 2022 9

Table 4: Annual Inventories of IT Assets That May Process and Store Classified Information, as of September 2022 10

Accessible Data for Table 4: Annual Inventories of IT Assets That May Process and Store Classified Information, as of September 2022..... 11

Figure

Figure 1: Total IT Assets in OIG Review Not Inventoried in Fiscal Year 2020..... 5

Accessible Data for Figure 2: Total IT Assets in OIG Review Not Inventoried in Fiscal Year 2020 5

Abbreviations

ERM	Enterprise Risk Management
FMS	Facilities Management and Services
FMS/PB	Facilities Management and Services/Property Branch
FY	Fiscal Year
Framework	GAO’s Fraud Risk Management Framework
IO	Infrastructure Operations
IT	Information Technology

Introduction

Starting in March 2020, GAO shifted to a remote operating posture to help protect employees during the COVID-19 pandemic. This posed operational challenges to GAO's Infrastructure Operations (IO) office, which has responsibility for effective stewardship of information technology (IT) assets, in performing its annual inventory of accountable personal property—which includes IT assets such as laptops, hard drives, scanners, mobile storage devices, and printers. These assets may process and store information under the authority or control of GAO that requires protection from unauthorized disclosure, including classified information.¹ Additionally, these assets could be easily lost, stolen, or converted to personal use. Protection of information under the authority and control of GAO is important because unauthorized disclosure can harm important interests, such as national security; law enforcement; personal privacy; proprietary commercial rights; and GAO's accountability, reliability, and integrity. Annual inventory is the primary control that GAO has over these assets and, by extension, the sensitive or classified information that these devices may process or store.

Objective, Scope, and Methodology

We examined IO's inventory control over certain IT assets that may process or store sensitive or classified information during the onset and height of the pandemic. These items have the potential for national security, privacy, and other major risks as well as reputational, mission, and fraud risks² if lost, stolen, or otherwise missing. We spoke with IO officials and other stakeholders to obtain information and documentation related to IO's annual inventory activities in fiscal year (FY) 2020 and 2021. For our review, we chose 5,643 in-use and in-stock accountable IT assets assigned to GAO headquarters and field offices.³ These assets were assigned to:

- Employees and contractor staff
- Defined use areas, such as stock areas
- Limited access areas, such as secure rooms
- Off-site offices, such as audit sites
- Common spaces

For each IT asset selected for review, we analyzed the relevant property records in GAO's Asset Manager to determine the extent to which IO verified the asset and its related barcode number, assignment, and location during FY 2020 and 2021. For a full description of our scope and methodology, please see appendix I.

¹Classified information shall be processed only on approved information systems. Source: GAO Directive 0910.1-02, *Information Security Requirements for Classified Information*, Chapter 9, para.2.a (July 1, 2013). These assets are identified by distinct personal property custodial codes in the GAO's Asset Manager (GAO's system of record for all accountable assets).

²Fraud risk exists when individuals have an opportunity to engage in fraudulent activity, have an incentive or are under pressure to commit fraud, or are able to rationalize committing fraud. When fraud risks can be identified and mitigated, fraud may be less likely to occur.

³We did not include new IT assets IO received and added to GAO's Asset Manager after the FY 2021 annual inventory.

We conducted this performance audit from June 2022 through March 2023 in accordance with generally accepted auditing standards. 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Background

Accountable property is nonexpendable personal property with an expected useful life of normally 1 year or longer that IO, in collaboration with other internal stakeholders, determines should be tracked in GAO’s property records based on the item’s acquisition cost and sensitivity. GAO determines its appropriate capitalization threshold based on acquisition cost. All capitalized property is accountable. Because certain IT assets are sensitive or may have security implications, these assets—such as laptop and desktop computers, mobile computing devices, data storage devices, and scanners and printers—are considered accountable regardless of acquisition cost or value. GAO’s order for control of capitalized and other accountable property sets accountability thresholds and controls for its personal property, as noted in Table 1 below.⁴

Table 1: Accountable Personal Property Classification, Acquisition Threshold, and Control

Personal property classification	Acquisition cost threshold	Control
<i>Capitalized</i> Accountable	\$15,000 or >per item or > \$150,000 for bulk buys	Capitalized accountable personal property is recorded in a general ledger fixed-asset account and reported on GAO’s annual financial statement. This property has a serial number, is tagged with a unique GAO identifier (barcode), and is to be inventoried annually.
<i>Noncapitalized</i> Accountable	>\$1,000 but <\$15,000	Noncapitalized accountable personal property has a serial number, is tagged with a unique GAO identifier (barcode), and is to be inventoried annually.

Source: OIG analysis of GAO policies for controlling nonexpendable personal property. | OIG-23-1.

Roles and Responsibilities for Annual Inventory of Accountable Property

GAO’s personal property management policy designates property accountability and inventory responsibilities to officials within IO, and management of assigned property to personal property custodian officials, as shown in Table 2.

⁴GAO Order 0621.3, *Control of Capitalized and Other Accountable Personal Property* (August 3, 2012).

Table 2: GAO Policy Governing Designations and Responsibilities for Accountable Personal Property

Designations	Responsibilities
IO	<ul style="list-style-type: none">• Develops policies for and administers control over GAO's property management program• Maintains the official property control records• Prescribes procedures, methods, and forms for property acquisition, utilization, transfer, maintenance, and disposal or retirement• Classifies the property for both management and accounting purposes• Administers and maintains the GAO property control and accountability system, as prescribed by IO and GAO's accountable personal property order• Designates custodial areas and Personal Property Custodial Officers for accountable property due to the nature of the property or its physical location• Ensures inventories of personal property are conducted within all GAO organizational units once a year
Personal Property Custodial Officers	Manage accountable property as assigned by IO

Source: OIG analysis of GAO accountable personal property policies | OIG-23-1.

The importance of adequately accounting for personal property, including IT assets held by GAO, stems primarily from the fact that public funds are invested in these resources. Among other things, this investment creates the need for management to account for these resources and use all appropriate techniques, such as conducting inventories, to manage them properly, efficiently, and effectively.

Overview of Annual Inventories of Accountable Personal Property

IO annually conducts an inventory of all accountable property, either on-site at GAO headquarters, field offices, and audit site locations; or via email correspondence with employees and contractor staff to verify information regarding the assets assigned to them.⁵

Annually, IO verifies assets assigned to

- GAO headquarters and field office defined-use areas through a combination of email correspondence and physically locating each accountable property item
- Off-site locations, such as audit sites, through e-mail correspondence, and contact with the relevant property custodians for these assets and locations as needed
- Individual GAO headquarters and field office employees and contractor staff, including expanded telework participants, through email correspondence requesting barcode numbers and locations for all accountable property assigned to

⁵IO's annual personal property inventory procedure provides that asset verification based on email outreach meets GAO's requirements for an inventory.

them. The inventory team do not enter individual workspaces to physically locate or scan asset barcodes for these assets

For the majority of FY 2020 and 2021, GAO headquarters and field offices operated in a maximum telework posture in response to the COVID-19 pandemic.⁶ During these years, key policies and procedures established by GAO to control personal property, including email verification, provided IO with substantial latitude in conducting inventories.

Risk Assessment Actions Could Inform Inventory Activities during Future Disruptions

IO Did Not Leverage Existing Virtual Methods to Inventory IT Assets in 2020

In mid-May 2020, IO cancelled all inventory activities for FY 2020, including the activities that did not require face-to-face interactions and were conducted virtually in FY 2019. IO officials provided two primary justifications for their decision.

- First, almost 40 percent of GAO's 18,600 accountable assets were physically located in fixed areas of GAO facilities; limited-access areas, such as secure rooms; and offsite locations. Once GAO shifted its operating posture, the expectation was that staff would enter work sites rarely, if at all—making it difficult to conduct on-site inventories.
- Second, IO officials identified potential challenges related to their ability to inventory the remaining 60 percent of other property—which included IT assets—assigned to employees who were working remotely. Specifically, officials concluded that barcode verification would likely be difficult for these assets given that remote workers might not have possession (physical custody) of assets assigned to them.⁷

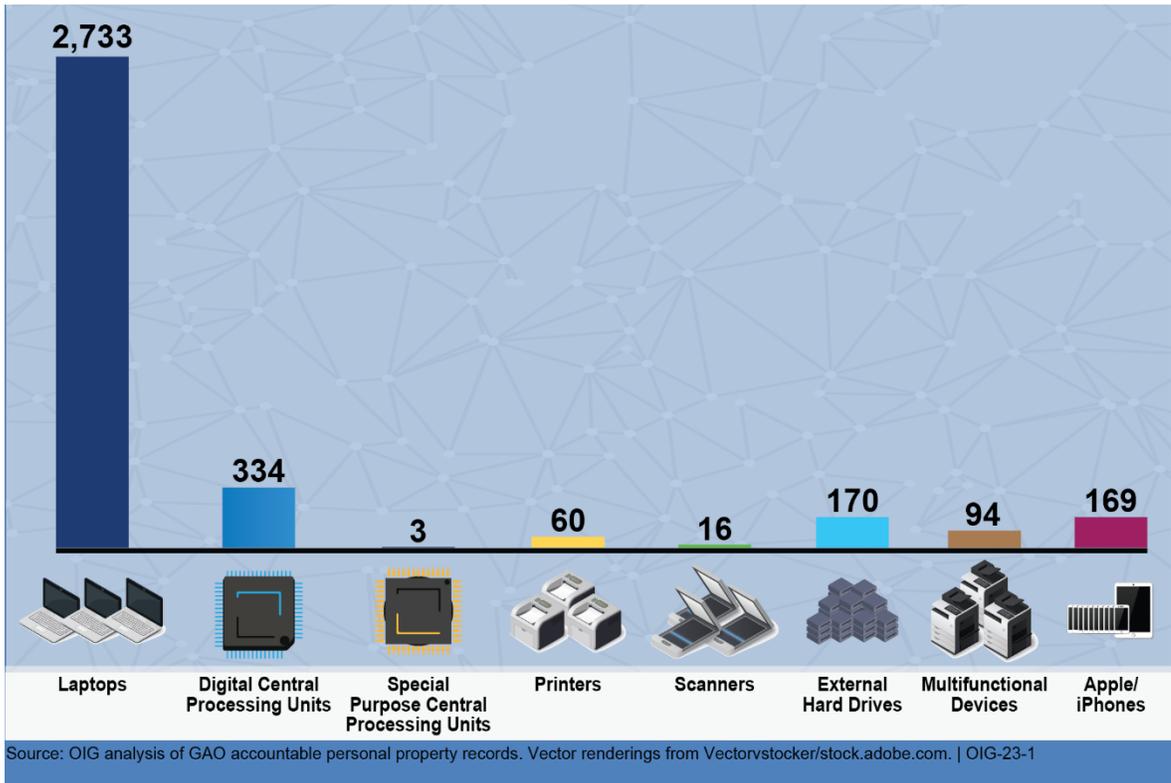
Property records showed that the barcode numbers, assignments, and locations of 3,579 IT assets included in our review that had been inventoried in FY 2019 were not inventoried in FY 2020.⁸ These IT assets may process or store sensitive or classified information under the authority or control of GAO that requires protection from unauthorized disclosure. Figure 1 shows the total number and type of IT assets not inventoried in FY 2020.

⁶In early August 2021, GAO reopened all of its office locations for voluntary re-entry.

⁷In a communication to all staff on March 13, 2020, GAO authorized all teleworking employees to take their GAO-issued IT assets to their alternate worksite to facilitate remote work. In a March 6, 2020 communication regarding telework readiness, GAO reminded employees with telework agreements to take home their GAO-issued laptops daily, among other things.

⁸FY 2020 inventory dates recorded for 23 IT assets for the most part represented dates the property records were updated to reflect follow-up activities for items not located during the FY 2019 inventory.

Figure 1: Total IT Assets in OIG Review Not Inventoried in Fiscal Year 2020



Accessible Data for Figure 2: Total IT Assets in OIG Review Not Inventoried in Fiscal Year 2020

IT Asset	IT Asset Total
Laptops	2,733
Digital Central Processing Units	334
Special Purpose Central Processing Units	3
Printers	60
Scanners	16
External Hard Drives	170
Multifunctional Devices	94
Apple/iPhones	169
Total	3,579

Source: OIG analysis of GAO accountable personal property records. | OIG-23-1

In explaining the decision to suspend all FY 2020 inventory activities, senior IO officials stated that IO management consensus was they had no way to conduct an inventory. In cancelling all inventory activities, however, IO did not leverage its existing inventory procedures that could have been performed through email verification to account for the IT assets assigned to specific individuals within GAO. Specifically, IO’s inventory procedures at the time provided for the use of email correspondence to confirm and document the

barcode number and location of each IT asset assigned to an individual.⁹ This inventory procedure was particularly important in light of the fact that GAO authorized all teleworking employees to take their GAO-issued IT assets to their alternate worksite to facilitate employees' ability work remotely early in the pandemic. Upon doing so, employees became responsible for the transportation and safeguarding of the government-issued equipment to alternative work locations and back to the office upon their return.¹⁰

IO did not assess the impact of the cancelled inventory on IT asset fraud risks

*Federal Internal Control Standards*¹¹ require managers to consider the potential for fraud when identifying, analyzing, and responding to risks as part of their internal control activities. GAO's *Fraud Risk Management Framework* (the Framework) identifies leading practices for planning and conducting fraud risk assessments.¹² According to the Framework, agencies should conduct risk assessments and document them in a fraud risk profile—and update those assessments and profiles when there is a change in a program or operating environment.¹³ The leading practices described in the Framework are meant to provide additional guidance for implementing requirements contained in *Federal Internal Control Standards*.

We reviewed GAO's FY 2020 fraud risk profile for IT assets. Based on the fraud risk assessment, IO and internal stakeholders identified fraud risks related to the inventory of and accounting for IT assets and controls to address them.¹⁴ Conducting an annual inventory was one of the existing antifraud controls in place to reduce the likelihood and impact of specific IT asset fraud risks. Notably, the fraud risk profile stated that the annual inventory had been postponed due to changes in GAO's operating status and was not expected to be completed by the end of the fiscal year. The profile, however, reflected that the cancelled annual inventory continued to effectively reduce identified IT fraud risks to lower levels. Based on the Framework, the cancellation of inventory activities should have prompted a new or revised IT asset fraud risk assessment and profile that reexamined the likelihood, impact, and significance of changes to existing IT fraud risks.

IO senior officials indicated they considered the risk low, given that employees were, for the most part, not regularly entering GAO office spaces. The officials stated that they accepted their property management professionals' assessment that inventory for FY2020

⁹Facilities Management and Services (FMS) Standard Operating Procedure—FMS/PB-2: *GAO Annual Personal Property Inventory*.

¹⁰https://intranet.gao.gov/covid-19/services/covid19_services/it_equipment.

¹¹GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 10, 2014).

¹²GAO, *A Framework for Managing Fraud Risks in Federal Programs*, [GAO-15-593SP](#) (Washington, D.C.: July 2015).

¹³According to the Framework, a fraud risk profile is an essential piece of an overall antifraud strategy. The profile includes the analysis of the types of internal and external fraud risks facing the program, their perceived likelihood and impact, managers' risk tolerance, and the prioritization of risks.

¹⁴For the assessment, a cross-functional team represented by subject matter experts across GAO identified fraud risks related to the inventory of and accounting for IT assets and identified responses. According to the profile, stakeholder offices were responsible for reevaluating identified fraud risks on a regular basis, or at least annually.

would be challenging. However, the officials did not recall whether any fraud risk assessment of IT assets was considered before deciding to cancel the inventory.

According to the fraud risk profile for IT assets, the internal owners responsible for addressing the fraud risks were expected to reevaluate identified fraud risks on a regular basis, or at least annually. Further GAO Order 0201.3 *Management's Responsibility for Internal Control* states that managing directors and office heads are primarily responsible for establishing, monitoring, and improving internal control. As noted, fraud risk was not considered in making the decision to cancel inventory activities due to the pandemic and then not reevaluated to consider the effect of not having the principal existing antifraud control in place.

As the responsible property management risk owner, IO lacks procedures for updating or revising IT asset fraud risk assessments and profiles when significant changes occur due to emergencies or other unplanned events, which is inconsistent with the Framework.

Establishing procedures to update or revise IT asset fraud risk assessments and profiles when unexpected or unanticipated events occur could help ensure IO makes informed risk-based decisions regarding inventory activities.

IO Inventoried a Sample of Assets in 2021 that Omitted Certain IT Assets

GAO's order for controlling nonexpendable personal property requires IO to develop inventory procedures prior to conducting the inventory each year. In FY 2021, IO's inventory procedures required an inventory of all accountable property agency-wide, including IT assets assigned to GAO headquarters and field office areas; off-site locations, such as audit sites; and individual employees and contractor staff.¹⁵ Notably, GAO's FY 2021 fraud risk profile for IT assets documented its planned reliance on IO's annual inventory to manage certain fraud risks identified.

IO inventoried a sample of GAO's accountable personal property in FY 2021. Our analysis of accountable property records maintained by IO for 5,374 IT assets that may process and store sensitive information showed that less than 20 percent (1,035) were inventoried in FY 2021 and almost 15 percent (803) did not have an inventory date. (Table 3)

¹⁵FMS Standard Operating Procedure—FMS/PB-2: *GAO Annual Personal Property Inventory*.

Table 3: Annual Inventories of IT Assets That May Process and Store Sensitive Information, as of September 2022

Property Category	FY 2019	FY 2021	No Inventory Date	Total
 Laptops	2,694	414	392	3,500
 CPUs	332	321	13	666
 Special Purpose CPUs	3	6	0	9
 Printers	60	56	26	142
 Scanners	16	14	0	30
 External Hard Drives	168	118	23	309
 Multifunctional Devices	94	37	9	140
 Apple/iPhones	169	69	340	578
Total	3,536	1,035	803	5,374

Source: OIG analysis of GAO accountable personal property records. Vector renderings from Vectorstocker/stock.adobe.com. | OIG-23-1

Accessible Data for Table 3: Annual Inventories of IT Assets That May Process and Store Sensitive Information, as of September 2022

Property Category	FY 2019	FY 2021	No Inventory Date	Total
Laptops	2,694	414	392	3,500
CPUs	332	321	13	666
Special purpose CPUs	3	6	0	9
Printers	60	56	26	142
Scanners	16	14	0	30
External hard drives	168	118	23	309
Multifunctional devices	94	37	9	140
Apple/iPhones	169	69	340	578
Total	3,536	1,035	803	5,374

Source: OIG analysis of GAO accountable property records. | OIG-23-1.

In addition, while the majority (162) of the remaining 246 IT assets that were designated as classified equipment in GAO’s property records were inventoried in FY 2021, over 15 percent (41) did not have an inventory date. (Table 4)

Table 4: Annual Inventories of IT Assets That May Process and Store Classified Information, as of September 2022

Property Category	FY 2019	FY 2021	No Inventory Date	Total
 Laptops	39	117	23	179
 CPUs	2	31	17	50
 Special Purpose CPUs	0	0	0	0
 Printers	0	1	0	1
 Scanners	0	3	0	3
 External Hard Drives	2	7	1	10
 Multifunctional Devices	0	3	0	3
 Apple/iPhones	0	0	0	0
Total	43	162	41	246

Source: OIG analysis of GAO accountable personal property records. Vector renderings from Vectorstocker/stock.adobe.com. | OIG-23-1

Accessible Data for Table 4: Annual Inventories of IT Assets That May Process and Store Classified Information, as of September 2022

Property Category	FY 2019	FY 2021	No Inventory Date	Total
Laptops	39	117	23	179
CPUs	2	31	17	50
Special purpose CPUs	0	0	0	0
Printers	0	1	0	1
Scanners	0	3	0	3
External hard drives	2	7	1	10
Multifunctional devices	0	3	0	3
Apple/iPhones	0	0	0	0
Total	43	162	41	246

Source: OIG analysis of GAO accountable property records. | OIG-23-1.

IO did not document any risk assessment performed for the purpose of sample selection

In an April 2021 memo to GAO’s Office of Internal Control, IO explained that it would resume modified inventory activities in FY 2021. According to the memo, IO developed a risk-based inventory plan to restart inventory activities at GAO headquarters only. To determine which assets to include in the modified inventory, IO said it considered agency-wide property risk vulnerabilities, property sensitivities/security, property values, fixed areas accessible to the inventory team, and ways to complete inventory activities by September 30, 2021. While the memo broadly outlined property risk considerations, IO provided no documentation to indicate consideration of the:

- Most significant property risks IO had identified and assessed, such as IT assets that had not been inventoried since FY 2019, or did not have an inventory date.
- Magnitude of those risks, including fraud risks, for certain IT assets (e.g., their likelihood and potential impact)
- Alternatives to GAO’s annual inventory activities that IO had evaluated to address those risks
- Rationale for including property such as cafeteria, fitness center, and mailroom equipment in the modified inventory but excluding most of the IT assets discussed earlier

IO lacks procedures requiring appropriate risk-based assessments to be completed when planning to implement an alternative to GAO’s full annual inventory to ensure samples are targeted to the highest risk assets, such as IT assets that can process and potentially store sensitive or classified information.

GAO Order 0201.3 *Management’s Responsibility for Internal Control* states that managing directors and office heads are primarily responsible for establishing, monitoring, and improving internal control. GAO’s Enterprise Risk Management (ERM) framework

identifies essential elements for ERM and good practices that illustrate them.¹⁶ The framework suggests several risk assessment best practices that IO could have applied to its decisions regarding inventory activities, including

- Examining factors, such as potential events which could affect activities and evaluating the risks based on likelihood of occurrence and impact
- Identifying alternative approaches in response to assessed risks and evaluating the alternatives to select the most appropriate strategy to manage the risks
- Documenting the risk mitigation decisions and rationale to support them

Detailed and documented procedures to implement an alternative to GAO's required full annual inventory could help ensure that the appropriate risk-based assessments are completed and samples are targeted to the highest risk IT assets that may process or store sensitive or classified information.

Conclusions

An annual inventory is the primary control that GAO has over IT assets and, by extension, the sensitive and classified information that these devices may store. Establishing procedures to update or revise IT asset fraud risk assessments and profiles when unexpected or unanticipated events occur, such as disruptions to GAO's operating posture, could help ensure IO makes informed risk-based decisions regarding inventory activities. In addition, procedures to implement an alternative to GAO's full annual inventory requirement could help IO ensure that the appropriate risk-based assessments are completed and samples are targeted to the highest risk IT assets that may process or store sensitive or classified information.

Recommendations for Executive Action

We are making two recommendations to the Comptroller General:

The Acting Infrastructure Operations Managing Director should develop and document procedures to update or revise information technology asset fraud risk profiles when unexpected or unanticipated events occur, such as operating posture disruptions or changes to GAO's telework program.

The Acting Infrastructure Operations Managing Director should develop and document procedures to ensure the appropriate risk-based assessments are completed when planning to implement an alternative to GAO's full annual inventory to ensure samples are targeted to the highest risk information technology assets, such as those that may process or store sensitive or classified information.

¹⁶GAO, *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk*, [GAO-17-63](#) (Washington, D.C.: Dec. 1, 2016). According to the framework, ERM is a forward-looking management approach that allows agencies to assess threats and opportunities that could affect the achievement of their goals.

Agency Comments

The Inspector General provided GAO with a draft of this report for review and comment. In its written comments, reprinted in appendix II, GAO concurred with the recommendations and indicated that it had actions underway to address them.

Appendix I: Objective, Scope, and Methodology

This report addresses the extent to which GAO's Infrastructure Operations (IO) office established effective inventory control over information technology (IT) assets authorized to process or store sensitive or classified information during the pandemic. The audit focused on the FY 2020 and 2021 inventories of selected assets. At the time OIG's engagement was initiated, IO had not concluded its limited FY 2022 inventory of these assets. We excluded the FY 2022 inventory from this assessment because IO had not completed the inventory by the start of our engagement.

To address our objective, we reviewed and analyzed GAO's property management order and procedures that establish control and responsibilities for tracking the custody and location of accountable personal property and completing GAO's annual property inventory of these assets. We spoke with IO officials and other stakeholders to obtain information and documentation related to annual inventory activities in FY 2020 and 2021.

We reviewed GAO's Enterprise Risk Management Profiles, as of September 2020 and September 2021, to determine the extent to which GAO (1) identified and assessed potential areas of significant risk related to property management during the pandemic and (2) assessed IO mission readiness and operations specific to property management.

In addition, we reviewed GAO's FY 2020 and 2021 Fraud Risk Assessments of IT Assets to determine the extent to which GAO deliberated and documented its consideration of property management activities in the pandemic operating environment and specifically its decision not to inventory IT assets that may process or store sensitive or classified information.

We analyzed data in Asset Manager—GAO's official system of record for its personal property inventory—to identify the number and types of IT assets recorded in the agency's official property records, as of September 2022. We then analyzed property codes to identify accountable personal property that may process or store sensitive or classified data. These types of assets included laptops, digital central processing units, tablets and smart phones, and peripheral equipment such as external data storage devices, scanners, and printers that were assigned either to certain locations in GAO buildings or to specific individuals. Because IO did not maintain a detailed list of all IT assets in GAO's inventory that process classified information, we analyzed Asset Manager personal property custodial codes to identify those assets designated as classified data processing equipment.

For the IT assets identified, we analyzed assignment designations to identify assets that, as of September 2022, were

- In-use (i.e., assigned either to certain locations in GAO buildings or to specific individuals)
- In-stock (i.e. held in various GAO headquarters and field office stock areas for future use)
- Returned for maintenance or to the supplier
- Designated as missing

For our review, we chose the 5,643 in-use and in-stock IT assets assigned to GAO headquarters and field offices. These assets were further assigned to:

- Employees and contractor staff

- Defined use areas, such as stock areas
- Limited access areas, such as secure rooms
- Off-site offices, such as audit sites
- Common spaces

To determine whether barcode numbers and inventory dates recorded in Asset Manager for the IT assets chosen for review were reliable, we reviewed electronic inventory records that IO maintained for IT assets that were verified in the FY 2021 inventory and validated the spreadsheet identifying assets inventoried. We determined that the data we obtained were sufficiently reliable for the purpose of our review.

For each IT asset chosen for review, we analyzed the related property records in GAO's Asset Manager to determine the extent to which IO verified the asset and its related barcode number, assignment, and location during FY 2020 and 2021.

We conducted this performance audit from June 2022 through March 2023 in accordance with generally accepted government auditing standards. 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix II: Comments from the U.S. Government Accountability Office



Memorandum

Date: May 24, 2023

To: Inspector General, L. Nancy Birnbaum

From: Acting Managing Director, Infrastructure Operations – Lisa Binckes

Subject: Response to Draft Report on Information Technology Assets: Risk Assessment Actions Could Inform Inventory Activities during Future Disruptions (OIG-23-1)

Thank you for the opportunity to review and comment on your draft report, *Information Technology Assets: Risk Assessment Actions Could Inform Inventory Activities during Future Disruptions (OIG-23-1)*. Infrastructure Operations (IO) concurs with the OIG's draft report recommendations. Below are GAO's comments on the draft report and action plan to address the recommendations.

It is important to note that IO considered the configuration and capabilities of GAO laptops as part of the risk mitigation in not conducting a full annual inventory in FY 2020 and FY 2021. GAO laptops have little intrinsic worth or book value and are configured with a very lightweight operating system called IGEL that does not allow staff to save data locally on the laptop, thereby limiting the ability to store information overall. This system allows staff to access the VDI network only, where information is stored in a data center in the Headquarters building and not the laptops. Additionally, staff cannot save files to laptop hard drives, and as a result no files or data is stored on these laptops.

Only a small percentage of tightly controlled GAO laptops use an operating system allowing staff to save files to the hard drive. These laptops are fully disk-encrypted and can only be accessed using two-factor authentication with a secure personal identification number and a physical RSA token that must be plugged into the laptop. This two-factor authentication login and encryption prevents unauthorized access to GAO laptops. As a result, although annual inventory is a key antifraud control activity—specifically for employee or contractor theft of equipment—IO deemed the overall impact on the IT asset fraud risk the same due to the inability to store information locally on the laptops.

As the report notes, IO had to pivot its inventory operations to manage in a remote environment during the unprecedented COVID-19 pandemic, with the first priority of protecting the health and safety of its employees. This audit began in late June 2022 and focused on the time period at the beginning of the COVID-19 pandemic and we would like to highlight our inventory practices, as well as the improvements that were made during the pandemic.

From March 2020 to August 2021, GAO headquarters remained in a telework status due to the pandemic. During this period, GAO field offices remained closed. GAO did evaluate the risk of suspending inventory activities during the period. IO coordinated with stakeholders and leadership on annual inventory activities for FY 2020 and FY2021. IO provided the Office of Internal Control with a property inventory plan describing modifying the annual inventory process due to the pandemic for each of these fiscal years. IO also discussed with CAO leadership suspending inventory in FY 2020 and modifying inventory in FY 2021 as part of several contingency planning briefings during the pandemic.

IO also considered the agency's operating status as part of its risk assessment for not conducting a full annual inventory for FY 2020 and FY 2021. While IO had existing inventory procedures to verify barcodes and locations through email correspondence to account for IT assets assigned to specific individuals within GAO, this method was primarily used prior to the pandemic for expanded teleworkers, which was only a small percentage of the overall workforce.

Notably, as the course of the pandemic evolved, IO increased its annual inventory efforts accordingly. For example, in FY 2022, IO conducted an inventory of all classified laptops assigned to GAO employees, which utilized an in-person verification process. Also, in January 2022 GAO began to replace old laptops with new laptops which required employees to turn in their old laptops as part of the process. Additionally, as part of FY 2023 inventory, IO has developed a plan incorporating a variety of processes to conduct an inventory of assigned laptops, monitors and cellphones. The plan will also be in-place in the instance of another National Emergency.

Recommendation 1:

Develop and document procedures to update or revise IT asset fraud risk profiles when unexpected or unanticipated events occur, such as operating posture disruptions or changes to GAO's telework program.

GAO Response:

IO concurs with the recommendation. IO is developing and documenting its standard procedures for updating or revising IT asset fraud risk profiles when unexpected or unanticipated events occur that result in a change in the annual inventory program or operating environment. We expect to complete these actions by September 30, 2023.

Recommendation 2:

Develop and document procedures to ensure that the appropriate risk-based assessments are completed when planning to implement an alternative to GAO's full annual inventory to ensure samples are target to the highest-risk IT assets.

GAO Response:

IO concurs with the recommendation. IO is developing and documenting its standard procedures to complete appropriate risk-based assessments and use these assessments to target high-risk IT assets when planning to implement an alternative to GAO's full annual inventory. We expect to complete these actions by September 30, 2023.

cc: Karl Maschino, Chief Administrative Officer / Chief Financial Officer
Paul Johnson, Deputy Chief Administrative Officer
Bill Anderson, Controller / Deputy Chief Financial Officer
Linda Hong, Director of Facilities Management and Services

Accessible Text for Appendix II: Comments from the U.S. Government Accountability Office

Memorandum

Date: May 24, 2023

To: Inspector General, L. Nancy Birnbaum

From: Acting Managing Director, Infrastructure Operations – Lisa Binckes

Subject: Response to Draft Report on Information Technology Assets: Risk Assessment Actions Could Inform Inventory Activities during Future Disruptions (OIG-23-1)

Thank you for the opportunity to review and comment on your draft report, Information Technology Assets: Risk Assessment Actions Could Inform Inventory Activities during Future Disruptions (OIG-23-1). Infrastructure Operations (IO) concurs with the OIG's draft report recommendations. Below are GAO's comments on the draft report and action plan to address the recommendations.

It is important to note that IO considered the configuration and capabilities of GAO laptops as part of the risk mitigation in not conducting a full annual inventory in FY 2020 and FY 2021. GAO laptops have little intrinsic worth or book value and are configured with a very lightweight operating system called IGEL that does not allow staff to save data locally on the laptop, thereby limiting the ability to store information overall. This system allows staff to access the VDI network only, where information is stored in a data center in the Headquarters building and not the laptops. Additionally, staff cannot save files to laptop hard drives, and as a result no files or data is stored on these laptops.

Only a small percentage of tightly controlled GAO laptops use an operating system allowing staff to save files to the hard drive. These laptops are fully disk-encrypted and can only be accessed using two-factor authentication with a secure personal identification number and a physical RSA token that must be plugged into the laptop. This two-factor authentication login and encryption prevents unauthorized access to GAO laptops. As a result, although annual inventory is a key antifraud control activity—specifically for employee or contractor theft of equipment—IO deemed the overall impact on the IT asset fraud risk the same due to the inability to store information locally on the laptops.

As the report notes, IO had to pivot its inventory operations to manage in a remote environment during the unprecedented COVID-19 pandemic, with the first priority of protecting the health and safety of its employees. This audit began in late June 2022 and focused on the time period at the beginning of the COVID-19 pandemic and we would like to highlight our inventory practices, as well as the improvements that were made during the pandemic.

From March 2020 to August 2021, GAO headquarters remained in a telework status due to the pandemic. During this period, GAO field offices remained closed. GAO did evaluate the risk of suspending inventory activities during the period. IO coordinated with stakeholders and leadership on annual inventory activities for FY 2020 and FY2021. IO provided the Office of Internal Control with a property inventory plan describing modifying the annual inventory process due to the pandemic for each of these fiscal years. IO also discussed with CAO leadership suspending inventory in FY 2020 and modifying inventory in FY 2021 as part of several contingency planning briefings during the pandemic.

IO also considered the agency's operating status as part of its risk assessment for not conducting a full annual inventory for FY 2020 and FY 2021. While IO had existing

inventory procedures to verify barcodes and locations through email correspondence to account for IT assets assigned to specific individuals within GAO, this method was primarily used prior to the pandemic for expanded teleworkers, which was only a small percentage of the overall workforce.

Notably, as the course of the pandemic evolved, IO increased its annual inventory efforts accordingly. For example, in FY 2022, IO conducted an inventory of all classified laptops assigned to GAO employees, which utilized an in-person verification process. Also, in January 2022 GAO began to replace old laptops with new laptops which required employees to turn in their old laptops as part of the process. Additionally, as part of FY 2023 inventory, IO has developed a plan incorporating a variety of processes to conduct an inventory of assigned laptops, monitors and cellphones. The plan will also be in-place in the instance of another National Emergency.

Recommendation 1:

Develop and document procedures to update or revise IT asset fraud risk profiles when unexpected or unanticipated events occur, such as operating posture disruptions or changes to GAO's telework program.

GAO Response:

IO concurs with the recommendation. IO is developing and documenting its standard procedures for updating or revising IT asset fraud risk profiles when unexpected or unanticipated events occur that result in a change in the annual inventory program or operating environment. We expect to complete these actions by September 30, 2023.

Recommendation 2:

Develop and document procedures to ensure that the appropriate risk-based assessments are completed when planning to implement an alternative to GAO's full annual inventory to ensure samples are target to the highest-risk IT assets.

GAO Response:

IO concurs with the recommendation. IO is developing and documenting its standard procedures to complete appropriate risk-based assessments and use these assessments to target high-risk IT assets when planning to implement an alternative to GAO's full annual inventory. We expect to complete these actions by September 30, 2023.

cc: Karl Maschino, Chief Administrative Officer / Chief Financial Officer

Paul Johnson, Deputy Chief Administrative Officer

Bill Anderson, Controller / Deputy Chief Financial Officer

Linda Hong, Director of Facilities Management and Services

Appendix III: OIG Contact and Staff Acknowledgments

OIG Contact

L. Nancy Birnbaum, (202) 512-5748 or birnbaum1@gao.gov

Staff Acknowledgments

Mary Arnold Mohiyuddin (Assistant Inspector General for Audit), Sandra Burrell (Assistant Director), Kendrick Johnson (Assistant Director), and Adriana Pukalski (Legal Counsel) made major contributions to this report. Other key contributors included Gregory Borecki, Melanie H.P. Fallow, Thomas Johnson, and Cynthia Taylor.

Appendix IV: Report Distribution

U.S. Government Accountability Office

Gene L. Dodaro – Comptroller General
Orice Williams Brown – Chief Operating Officer
Karl J. Maschino – Chief Administrative Officer/Chief Financial Officer
Edda Emmanuelli-Perez – General Counsel
Lisa Binckes – Acting Managing Director, Infrastructure Operations
Warren Simmons – Director, Security and Emergency Management
Linda Hong – Director, Facility Management and Services
Nikki Clowers – Managing Director, Congressional Relations
Chuck Young – Managing Director, Public Affairs
William L. Anderson – Controller/Deputy Chief Financial Officer
Adrienne C. Walker – Director, Office of Internal Control
Adebiyi A. Adesina – Special Assistant to the Controller
Jennifer Ashley – Special Assistant for Operational Initiatives

GAO Audit Advisory Committee

GAO Congressional Oversight Committees

OIG Mission

Our mission is to protect GAO's integrity through audits, investigations, and other work focused on promoting the economy, efficiency, and effectiveness in GAO programs and operations, and to keep the Comptroller General and Congress informed of fraud and other serious problems relating to the administration of GAO programs and operations.

Reporting Fraud, Waste, and Abuse in GAO's Internal Operations

To report fraud and other serious problems, abuses, and deficiencies relating to GAO programs and operations, you can do one of the following (anonymously, if you choose):

- Call toll-free (866) 680-7963 to speak with a hotline specialist, available 24 hours a day, 7 days a week.
- Visit GAO-OIG Listening Line

Obtaining Copies of OIG Reports and Testimonies

To obtain copies of OIG reports and testimonies, go to GAO's website: <https://www.gao.gov/ig> or <https://www.oversight.gov/reports>, maintained by the Council of Inspectors General on Integrity and Efficiency.