ADS 547

Property Management of Information Technology (IT)

Partial Revision Date: 08/05/2024
Responsible Office: M/CIO/ITO
File Name: 547_080524

Functional Series 500 – Management Services
ADS 547 – Property Management of Information Technology (IT)
POC for ADS 547: See ADS 501maa, ADS Chapters and Point of Contact List

Table of Contents

ADS 547 – Property Management of Information Technology (IT)

547.1 OVERVIEW

Effective Date: 11/20/2019

This chapter provides the framework for the worldwide property management of USAID's information technology (IT) assets. This chapter applies to all Bureaus, Independent Offices, and Missions (B/IO/Ms), and organizations conducting business for, and on behalf of, USAID through contractual relationships when using USAID IT assets. Throughout this chapter, the terms, "workforce" and "individuals," refer to individuals working for, or on behalf of, the Agency, regardless of hiring or contracting mechanism, who have physical and/or logical access to USAID facilities and information systems. This includes, but is not limited to United States Direct-Hire employees, Personal Services Contractors, Fellows, Participating Agency Service Agreements, and contractor personnel. Contractors are not normally subject to Agency policy and procedures as discussed in **ADS 501**. However, contractor personnel are included here by virtue of the applicable clauses in the contract related to Homeland Security Presidential Directive 12 (HSPD-12) and information security requirements.

IT assets include, but are not limited to: computers (government furnished equipment [GFE] laptops and desktops), software, voice over internet protocol (VoIP) phones (desk lines), computer monitors, mobile phones, tablets, printers, scanners, fax machines, peripherals (*e.g.*, computer memory, hard drives, keyboards, and cameras), infrastructure equipment (router, switch, hub, server, firewall, encrypter), tokens, portable storage devices (*e.g.*, USB drives (M/CIO approved encrypted USB drives), and portable hard drives.

Please note that some of the hyperlinks in the ADS can only be accessed on the USAID network (AIDNet).

547.2 PRIMARY RESPONSIBILITIES

Effective Date: 01/11/2024

a. The **Bureau for Management, Office of the Chief Information Officer (M/CIO)**, is responsible for Information Resources Management (IRM), as defined in the **E-Government Act of 2002**, **OMB Circular A-130**, and **OMB M-16-02**. M/CIO is also responsible for all CIO functions that are mandated by the **Clinger-Cohen Act of 1996**, the **Federal Information Technology Acquisitions Reform Act (FITARA) of 2014**, and the **Making Electronic Government Accountable By Yielding Tangible Efficiencies Act of 2016 (MEGABYTE Act)**. M/CIO designs, develops, issues, and implements property management policies, guidelines, and programs that are applicable to IT hardware and software.

b. The **Information Technology Property Management Officer (IT PMO)**: In USAID/Washington (USAID/W), the CIO is the IT PMO. The M/CIO IT PMO is authorized to delegate responsibility for the various other property management

functions to other officers (preferably members of the same staff), such as the Accountable Property Officer (APO) and the Property Disposal Officer (PDO) (see **ADS 518, Personal Property Management (Domestic)** and **ADS 534, Personal Property Management Overseas**, for more information).

The IT PMO is responsible for budgetary reporting to the Office of Management and Budget (OMB) and is responsible for accountability, receipt, storage, issuance, record keeping, inventory, reporting, and certification of all records and reports on IT assets within the Agency (see **ADS 549, Telecommunications Management**, **ADS 534, Personal Property Management Overseas**, and **14 FAM 411.2-2a and 2-b**).

In overseas locations, the **Executive Officer (EXO)** or **Agency Principal Officer** (if no EXO is assigned) serves as the Mission IT APO for IT assets, including leased IT assets. The EXO is responsible for all personal property management functions, including establishing internal policies and procedures for management and control of assigned personal property. The EXO is also responsible for maintaining an accurate inventory of IT assets and for providing that inventory to the M/CIO IT PMO to ensure that all USAID IT assets are accounted for. The EXO must provide M/CIO with support when IT asset information is required for data calls (*e.g.*, mobile phone usage (quantity of minutes, data and text messages)).

Both the EXO and the IT PMO must ensure that the policies and procedures outlined in this ADS chapter are implemented, and they must ensure compliance with Agency and government-wide authorities and guidelines (see **ADS 549**, **ADS 534**, and **14 FAM 411.2-1**).

c. The **Head of each Mission, Bureau, or Independent Office** appoints an organizational Property Custodian, who is charged with ensuring that all IT assets, including, but not limited to, computer hardware, software, and cloud services used by the organization are properly controlled in a manner aligned with M/CIO approved software (contact **ecm@usaid.gov** to determine if the proposed software is approved for use), **IT Standards**, and policies.

d. **USAID/W Property Custodians** oversee IT assets assigned to personnel in their organizations. Administrative Management Staff/Executive Management Team (AMS/EMT) Officers, or the individual designated by the Head of each Bureau or Independent Office, must ensure that all IT assets are assigned to an individual, and when not in use, are returned to M/CIO for storage, reassignment, or disposition (*e.g.*, Supervisory AMS Officers or AMS/EMT Officers).

e. The **Bureau for Management, Office of the Chief Information Officer, IT Operations Division (M/CIO/ITO)** manages the maintenance of all Agency government furnished equipment IT assets and IT infrastructure. M/CIO/ITO coordinates with relevant offices on inventories of available GFE and other necessary equipment for staff use in the Telework and Remote Work Program.

f. The **Agency workforce** is responsible for the appropriate care, proper custody, and efficient use of IT assets issued for individual use.

g. The **M/CIO Software Manager** manages Agency-wide commercial and commercial off-the-shelf (COTS) software agreements and licenses. The Software Manager must develop and implement strategies to address life-cycle phases and reduce duplication of software licenses throughout the Agency by 1) centrally managing software buys and reducing underutilization of software, 2) maintaining a continuous inventory of software licenses and tracking software usage, 3) consolidating redundant applications, and 4) maximizing the use of best-in-class solutions.

h. The **Bureau for Management, Office of the Chief Financial Officer, Central Accounting and Reporting Division (M/CFO/CAR)** records and accounts for capitalized asset(s), including IT capitalized software (see **ADS 629.3.6.1**).

M/CFO/CAR maintains the general ledger accounts for capitalized property and operating materials and supplies (see **ADS 629.3.6**), and issues a quarterly data call to the B/IO/Ms requesting information on capitalized property, including IT property, and operating material and supplies.

i. The **Bureau for Management, Office of Acquisition and Assistance (M/OAA)** is responsible for working with Operational Units when acquisitions include IT and for ensuring that the B/IO/M has secured M/CIO approval to move forward with the acquisition.

j. **B/IO/M Contracting Officer Representatives (CORs)** furnish information on IT property required for the M/CFO capitalized data call. CORs must include the following data:

- Cost of capitalized software for any system put in use since the last reporting cycle;
- Useful life of capitalized software;
- Cost of expensed software; and
- Enhancement costs to software (both capitalized and expensed) (see **ADS 629, Accounting for USAID-Owned Property and Internal Use Software** for further guidance on capitalization for internal use software).

547.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

547.3.1 Property Management of Information Technology (IT)

Effective Date: 11/20/2019

The USAID workforce must ensure that government furnished IT, including commercial

property leased or loaned to USAID, is used in accordance with the **FITARA** and the Information Technology Management Reform Act (see **Clinger-Cohen Act**). The other Federal laws and regulations cited in this ADS chapter, along with the policies and procedures detailed in this ADS chapter, are designed to ensure that IT assets are safeguarded against waste, loss, and misuse.

547.3.2 Management of Information Technology Devices (One Device)
Effective Date: 11/20/2019

Per **Executive Order (EO) 13589**, each member of the USAID workforce is eligible to be issued a single computer (a desktop or laptop) along with a minimum of a single monitor, relative to the employee's responsibilities, a keyboard, PIV reader, mouse, and docking station, if needed, and a desk phone. Assignment of mobile phones must be approved by B/IO/M leadership (see **ADS 549**). Users that were issued two monitors prior to September 30, 2019, are exempt from this requirement. For users with multiple monitors, any replacements or purchases of new monitors after September 30, 2019, must be approved through a reasonable accommodation request or a business waiver request.

B/IO Supervisory AMS Officers must contact the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** to request assignment of an IT asset.

Mission EXOs or System Managers must manage the assignment of the IT assets in Missions in accordance with M/CIO policy and in coordination with M/CIO.

Note: On a case-by-case basis, M/CIO may re-evaluate a user's business need requirements when more than one device and/or multiple accessories were issued prior to the issuance of the policy in this ADS chapter.

547.3.2.1 Reasonable Accommodation Request for an Additional Device
Effective Date: 11/20/2019

Individuals with disabilities who require an additional or specialized device or computer monitor must submit a **reasonable accommodation** request to the **USAID Office of Civil Rights and Diversity** Reasonable Accommodation Manager at **reasonableaccommodations@usaid.gov** (see **ADS 111, Procedures for Providing Reasonable Accommodation for Individuals with Disabilities**). Procurement, operations, and maintenance support for the second device and/or associated equipment must be approved and funded by the B/IO/M or through the M/MS maintained centralized fund for reasonable accommodations. Approved reasonable accommodation requests that support the assignment of a second device must be submitted to the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** by the requesting B/IO/M prior to procurement and installation for incorporation into the Agency IT inventory.

547.3.2.2 Business Waiver Request(s) for an Additional Device
Effective Date: 07/29/2022

If members of the workforce do not meet the reasonable accommodation criteria above, but still require an additional device or associated equipment in order to conduct Agency business, they may request an additional device by submitting a business waiver request (**https://www.usaid.gov/forms/aid-547-1**). The additional device/associated equipment must be approved by the individual's supervisor, B/IO/M leadership (Director or equivalent), and by M/CIO. Business waiver requests that are not related to a reasonable accommodation requirement must include a detailed justification that supports the request, as well as a business case that documents the negative operational impact if the business waiver request is not approved.

B/IO/M's may request a waiver from the Agency's One Device policy for members of the workforce who participate in the Agency Telework Program when the member of the workforce's assigned desk is in restricted space.

B/IO/M leadership must approve and submit the business waiver request(s) to the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov**. If approved, M/CIO will notify the B/IO/M AMS/EMT or EXO and provide a quote for the cost of the additional IT asset. The B/IO/M must approve the cost and initiate an order through an M/CIO-approved blanket purchase agreement (BPA). During the lifespan of the equipment, before it is disposed as outlined below, the additional IT asset (*e.g.*, desktop, laptop, tablet, or mobile phone) and associated equipment must be maintained by the requesting B/IO/M; the requesting B/IO/M is responsible for funding all annual maintenance costs. Note: Additional IT assets in USAID/W will be returned to the Agency inventory for reassignment when no longer in use by the designated user (this includes when the designated user transfers to an alternate Bureau or Independent Office in AID/W). The additional IT assets in a Mission will be returned to the Mission replacement inventory for reassignment when no longer in use by the designated user.

If the telework business waiver request is approved for users in restricted space, and the user has two devices (one for restricted space and one for unrestricted space) the user must not remove the restricted space device from the restricted space as it will be configured to comply with Agency security requirements in restricted space (see ADS 552.3.6.1). Users must ensure that the restricted space device is secured to the desk or in their workspace with a laptop chain. Failure to secure the restricted space device properly may be considered a security incident (see ADS 568).

Users must not bring/use Agency laptops that were issued for use in an alternate unrestricted work location into restricted space at any time. Doing so could cause a security incident (see ADS 568).

547.3.3 Procurement of IT Assets and Infrastructure
Effective Date: 11/20/2019

B/IO/Ms are prohibited from purchasing any equipment that is not through an M/CIO approved means for use on the Agency network. B/IO/Ms should contact M/CIO if the equipment required by the B/IO/M is not available on the Agency approved BPA for guidance on alternate purchasing options.

Effective in Fiscal Year (FY) 2018, B/IO/Ms must no longer purchase their own laptops and desktops. M/CIO centrally manages all purchasing of laptops and desktops. M/CIO works with B/IO/Ms to develop an annual IT refresh plan for their organization for laptops and desktops.

B/IO/Ms must only procure IT infrastructure equipment (*e.g.,* servers, routers, switches, network printers) that are currently approved for purchase by M/CIO (see **IT Standards**) and are available for purchase through a M/CIO Blanket Purchase Agreement (BPA) (please contact your B/IO/M Contracting Officer for guidance on methods of procurement). If the equipment is not on the IT Standards list, then the B/IO/M must obtain M/CIO approval prior to procurement. The B/IO/M must request this approval by submitting a **software and hardware approval request (SHARP)**. B/IO/Ms are prohibited from purchasing IT infrastructure equipment that is not approved by M/CIO.

Missions must work with M/CIO to develop and maintain an adequate replacement inventory for any IT assets including IT infrastructure equipment to ensure that damaged or lost/stolen equipment can be replaced in a timely manner. Missions must update their IT inventory as IT assets are replaced. Missions must also alert M/CIO when inventory IT infrastructure equipment is put in service to ensure that replacements are ordered in a timely manner.

In instances where B/IO/Ms have procured unapproved IT infrastructure equipment, they must not install the equipment on devices connected to AIDNET. M/CIO will not configure unapproved infrastructure equipment, will not provide technical support, and in most instances will require the B/IO/M to return or dispose of the unapproved equipment.

547.3.3.1 Local Purchasing of Information Technology Assets

Effective Date: 11/20/2019

In accordance with OMB A-130, Executive Order on Securing the Information and Communications Technology and Services Supply Chain, and National Institute of Standards and Technology Special Publication (NIST SP) 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, IT assets must not be procured locally or in-country. All IT assets must be purchased in the United States and through M/CIO supported acquisition vehicles where possible. M/CIO will maintain a Blanket Purchase Agreement (BPA) for procuring all approved IT assets.

USAID's approved IT asset BPA, centralized procurement, and U.S.-purchased IT asset acquisitions helps the Agency meet government-wide standards and requirements, and mitigates supply chain risks associated with information and communications

technology (ICT) products and services. Among other benefits, these acquisitions prevent the purchase of counterfeit equipment and protect the network from malicious software and hardware.

547.3.4 Assignment of IT Assets

Effective Date: 11/20/2019

All IT assets must be assigned to an individual user who takes physical possession and accountability of the device.

In addition, all IT assets must have a U.S. Direct-Hire, or designee, that accepts ownership of IT assets on behalf of their B/IO. By taking ownership, the Direct-Hire is responsible for managing the IT asset inventory. The Direct-Hire is responsible for reporting lost, damaged, or stolen equipment to M/CIO. In the event of unexplained/unresolved discrepancies, it is the responsibility of the Direct-Hire to resolve such problems. B/IOs are financially responsible for replacement of lost, damaged, or stolen endpoint devices (see **547.3.6** for guidance on individual responsibility for safeguarding IT assets).

In the continental United States (CONUS), the Supervisory AMS Officer is the U.S. Direct-Hire responsible for IT endpoint, shared, and infrastructure devices in the B/IO.

Outside the continental United States (OCONUS), the EXO or a designated USPSC is responsible for IT endpoint, shared, and infrastructure devices.

IT assets that are shared and considered “community” assets, such as printers/scanners or devices in conference rooms or desktops or laptops designated for “hoteling” offices/cubicles are the responsibility of the USAID/W Property Custodian or the Mission EXO or System Manager.

The B/IO/M AMS/EMT Officers or EXOs, or the designated USPSC, must ensure that all IT assets issued to their organizations are accounted for in the Agency IT inventory (see **547.3.5** for additional guidance). In instances where B/IO/M AMS/EMT Officers or EXOs are unable to locate an IT asset, they must immediately notify M/CIO that the equipment is missing (see **547.3.6** for further guidance).

Effective FY 2019, all OE-funded IT assets not in use will be stored or reassigned based on Agency needs.

547.3.4.1 Assignment of IT Assets in USAID/W

Effective Date: 11/20/2019

B/IOs must request assignment of end point devices (e.g., desktop computers, laptops, workstations, smartphones, tablets, and servers) and accessories by submitting a request to the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov**. In USAID/W, endpoint devices and accessories must only be requested when they can be

assigned to an individual and that individual has an assigned Bureau for Management, Office of Management Services Headquarters Management Division (M/MS/HMD) approved/authorized desk space (see **Space Management** for additional guidance) or is officially approved to work offsite. Government Furnished Equipment (GFE) will be issued to members of the workforce who work remotely upon request from the B/IO. Starting in FY 2019, M/CIO will implement an IT refresh plan for the Agency. B/IOs must provide M/CIO with an annual needs analysis to update the annual IT refresh plan no later than January 30 of each year through an annual data call.

If M/CIO has refreshed or scheduled a refresh of endpoint devices for your B/IO, the procurement of an additional device (outside of the one device policy) will require that a Business Waiver or 508 Compliance Waiver request be submitted and approved. The purchasing B/IO will be responsible for purchase and ongoing Operations and Management (O&M) costs.

547.3.4.2 Assignment of IT Assets in Missions
Effective Date: 11/20/2019

Missions must work with M/CIO to ensure that new IT assets are issued and incorporated into the authoritative IT Asset Management System (ITAM) for the correct users and that excess assets are removed from the network and disposed of in compliance with the M/CIO IT disposal process.

547.3.4.3 Emergency Distribution of IT Assets
Effective Date: 11/20/2019

Emergencies come in many forms (*e.g.*, hurricanes, tornadoes, earthquakes, floods, epidemics, terrorist attacks, etc.) that may displace USAID individuals. In the limited circumstance of an emergency that requires individuals to be relocated to an alternate location, M/CIO may assign IT assets to the relocated individuals. Requests for such assignments may come from an approved authority (AMS, EXO/System Manager (SM), etc.).

For OCONUS, Missions that have excess equipment available may make this equipment available to the affected Mission. When loaning equipment, Missions must update the ITAM for asset tracking purposes.

547.3.5 Agency Hardware Inventory
Effective Date: 11/20/2019

M/CIO is responsible for maintaining an up-to-date Agency-wide inventory of IT assets purchased by USAID, which includes IT assets purchased by USAID B/IO/Ms. M/CIO must barcode all accountable hardware purchased by USAID/W B/IOs and record the barcodes in the ITAM. If a Mission receives any IT assets without barcodes, the EXO must contact the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** to request barcodes, and ensure that the M/CIO approved barcode is affixed to the

asset and the details are reported to M/CIO for inclusion in the ITAM System.

B/IO/Ms and users are prohibited from removing M/CIO-issued barcodes from IT assets.

To ensure that the Agency's IT asset inventory is up-to-date, M/CIO will conduct an annual, full physical inventory for CONUS sites, and will coordinate the OCONUS inventory by working with Missions to complete and certify their physical inventory.

547.3.5.1 Role of Bureau Property Custodians (AMS/EMT Officers) and Mission Executive Officers (EXOs) in Inventory of IT Assets

Effective Date: 11/20/2019

M/CIO, in coordination with Property Custodians (*e.g.,* AMS/EMT Officers) in USAID/W and EXOs and System Managers (SMs) overseas, are the personnel responsible for conducting the annual physical inventory of IT assets to ensure the accuracy of IT resource records.

Physical inventory: For USAID/W, M/CIO conducts a physical inventory of all CONUS IT assets and compares it to IT assets listed in the ITAM system. For overseas locations, EXOs or the Mission Systems Manager are required to conduct an annual IT asset inventory and submit the list to M/CIO for comparison to the ITAM system. The AMS/EMT and/or EXO/SM must note any inconsistencies in ITAM. M/CIO will update the ITAM system accordingly, and report any lost or unaccounted for assets to M/CFO and the United States Computer Readiness Team (US CERT).

It is the B/IO/M's responsibility to ensure IT assets assigned to their organization are properly tracked. AMS/EMT Officers, EXOs/SMs, or individual staff may contact the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** to request an IT asset report. Individual staff not responsible for organizational IT assets may only request reports for IT assets that are assigned to them. See **547.3.6**, for guidance on missing or unaccounted for IT assets. AMS/EMT Officers in USAID/W and Mission EXOs must certify the results of the annual inventory.

In coordination with the M/CIO Asset Management Group, EXOs must conduct an IT asset inventory as follows:

- Certify IT Asset Inventory: EXO's must certify annually that they have reviewed the most recent Mission IT asset inventory.

- Annual full physical inventory: The EXO/SM must report the results to the M/CIO Asset Management Group via the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** by submitting a formal certification letter that lists all of the IT assets and includes a detailed description of all relevant information (barcodes and the individual assignee (see **547.3.3**) of the IT assets must be included).

- The EXO/SM must update the inventory of IT assets when a member of the Mission workforce joins or departs the Mission by updating the ITAM or contacting the M/CIO Asset Management Group via the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** to record the change.

Missions are required to participate in the USAID Asset Inventory, regardless of their use of the International Cooperative Administrative Support Services (ICASS) or Integrated Logistics Management System (ILMS).

See **547.3.3, Procurement of IT Infrastructure** and **547.3.4, Assignment of IT Assets** for guidance on procurement and assignment of IT assets to individual users. See **547.3.6, Safeguarding IT Assets** for guidance on reporting lost or stolen IT assets. See **547.3.16, Agency Software** for guidance on requirements related to software.

If equipment is determined to be surplus, M/CIO must prepare a report for the file, and include a full explanation of the known circumstances as well as a statement that the surplus is the result of the physical inventory. M/CIO must adjust the inventory accordingly and notify the Bureau for Management, Office of the Chief Financial Officer (M/CFO) of any situation affecting capitalized property (see **ADS 629, Accounting for USAID-Owned Property and Internal Use Software**).

547.3.5.2 Inventory of Agency IT Assets Used by Contractors in USAID/W and Overseas Locations

Effective Date: 11/20/2019

a. Contractors are required to maintain records for government property, including IT assets, in accordance with the terms and conditions of their contract. Government property includes government furnished property (GFP) and may include contractor acquired property (see **ADS 306mah** and **ADS 302** for additional policy and procedures and COR responsibilities regarding government property).

This section applies to both Operating Expense (OE)-funded and program-funded contracts, if either or both of the following conditions are met:

- The title of the IT assets reverts to the Agency at the end of the contract, or
- The title remains with the Agency.

b. B/IO/M's and local system managers may request that M/CIO issue Agency IT assets to contractors as GFP. USAID contractors may be held liable for any Agency IT asset lost or damaged by their employees. M/CIO will perform a yearly

physical inventory of IT assets located in USAID/W, including assets assigned to contractors. Missions are required to provide their IT asset inventory, including assets assigned to contractors, to the M/CIO Accountable Property Officer. Only IT assets that are published on the M/CIO **IT Standards** website and procured through M/CIO are authorized for use on AIDNet. Any other devices must access USAID corporate applications through remote access (**https://remoteaccess.usaid.gov**) using a remote access token (see **547.3.9, Secure Authentication Tokens (RSA Tokens)**).

c. When a contractor notifies the COR or CO that Agency IT assets are lost, stolen, destroyed, or damaged beyond economical repair, the CO or the COR must immediately notify the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** of the loss or damage. Upon notification of lost or stolen GFP, M/CIO must remove the equipment from the network. Once the COR has notified M/CIO of the damage or loss, they must assist the CO in determining contractor liability, if any, for the IT asset that was lost, stolen, or damaged (see **547.3.6**).

d. The COR must ensure that all USG IT assets are returned to M/CIO or the Mission EXO for inspection, sanitation, redisposition, and/or storage (see **547.3.4, Assignment of IT Assets** for further guidance) at the end of the contract, or upon termination of a contractor employee to whom the asset was assigned.

547.3.6 Internet of Things (IoT) Devices

Effective Date: 08/05/2024

The growth and daily use of network-connected devices, systems, and services comprising the IoT creates immense opportunities and benefits for USAID and our partners. Internet-connected devices enable seamless connections among people, networks, and physical services. Examples of IoT devices are computerized Internet-connected objects, such as networked security cameras, smart refrigerators, smart televisions, smart watches, drones, WiFi-capable automobiles, WiFi capable building management systems (such as thermostats, building monitoring, and fire control systems), and smart sensors, etc.

Laptops, tablets, mobile phones, and peripherals (e.g., wireless mice, keyboards, headphones, or monitors) are not considered IoT devices (see the **Agency Approved Product Catalog** for the list of approved peripherals).

While the benefits of the IoT are undeniable, IoT devices often lack cybersecurity functionality commonly present in conventional IT equipment (e.g., laptops). Sometimes, a lack of cybersecurity functionality in an IoT device or support from the manufacturer or supporting entities could introduce unacceptable levels of risk to the system, such as when an IoT device lacks a key device cybersecurity requirement.

Members of the Agency workforce must not connect IoT devices to Agency WiFi networks or to GFE (e.g., laptops, tablets, mobile phones), unless M/CIO has approved the IoT device to be connected to GFE or Agency wireless networks (see **Agency Approved Product Catalog (APC)** for list of approved IoT devices; the APC is accessible via the Agency intranet).

Per **OMB M-24-04** and the **Internet of Things (IoT) Act of 2020 (P.L. 116-207)**, Agencies "must have a clear understanding of the devices connected within their information systems to gauge cybersecurity risk to their missions and operations. This includes the interconnected devices that interact with the physical world—from building maintenance systems, to environmental sensors, to specialized equipment in hospitals and laboratories (see **OMB M-24-04** pages 5-8)."

USAID must maintain an authoritative Agency IoT Inventory that includes Agency IoT assets, including those that qualify as Operational Technology (OT) (see section **547.6**), to help ensure the cybersecurity posture of the Agency. An IoT inventory enables the Agency CIO and CISO to gain visibility over Agency connected devices and systems, supporting the application of appropriate controls (such as those set out in **NIST SP 800-82** and **NIST SP 800-213**), and make risk-based decisions about mitigating against cybersecurity threats.

IoT devices that are installed in co-located space or government facilities that are not managed by USAID (e.g., co-located Missions where the Department of State oversees the facilities) are not considered IoT that is used by the Agency. In this scenario, the IoT devices should not be submitted as part of the Agency IoT Inventory as they are not Agency assets. M/CIO must approve these IoT devices before they are connected to USAID networks (AIDNET or guest wireless). OUs must contact the M/CIO Service Desk at **cio-helpdesk@usaid.gov** to submit a request that non-USAID managed IoT devices installed in co-located space or government facilities be granted access to connect to USAID networks.

547.3.6.1 Agency IoT Inventory

Effective Date: 08/05/2024

OUs (typically the Business or System Owner, ISSO, USAID/W Property Custodians, or Mission Systems Managers) must participate in data calls from M/CIO for covered IoT/OT devices and assets. Per **OMB M-24-04** examples of covered IoT/OT devices are devices that are embedded with programmable controllers, integrated circuits, sensors, and other technologies for the purpose of collecting and exchanging data with other devices and/or systems over a network in order to facilitate enhanced connectivity, automation, and data-driven insights across devices and systems. OUs must provide (at a minimum) the following information upon request from M/CIO:

1. Asset Identification: All devices and systems that meet the provided definition of covered IoT assets.

2. Asset Description: Including make, model, and any relevant specifications or

configurations. Each asset should have a unique identifier, such as a serial or asset tag, to distinguish it from other assets.

3. Asset Categorization: Factor in the device's function, location, and criticality. Include the following information: a. Identification and/or description of specific Agency FISMA and HVA systems associated with the asset; and b. The physical location of the asset (e.g., building, floor, or room number).

4. Owner/Point of Contact: The individual or office responsible for the asset's management, administration, maintenance, and security.

5. Vendor/Manufacturer Information: Details about the vendor or manufacturer (e.g., contact information and support channels).

6. Software and Firmware Versions: Where available, record the installed software and firmware versions, including relevant patches or updates applied to the asset.

7. Network Connectivity, Integrations and API Information: Include any static IP addresses and interconnective communication with other devices (e.g., uncommon ports, protocols).

8. Security Controls: Describe alignment to requirements and controls (as appropriate), such as NIST Special Publication (SP) **800-213, IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements**, **SP 800-82,Guide to Operational Technology (OT) Security**, **SP 800-53, Security and Privacy Controls for Information Systems and Organizations**, and other standards and protocols.

OU Planners or CORs, Business and/or System Owners, and ISSOs must review **NIST SP 800-213** when exploring the adoption of an IoT device to help the OU assess risk and identify IoT device cybersecurity requirements for their use case(s).

IoT/OT use cases should address technical and cybersecurity considerations, including, but not limited to the following:

- What is the benefit of the IoT device and how will it be utilized?
- What data (e.g., personal data, confidential organizational/Federal Government data, environmental data) is collected/maintained by the IoT device?
- In what technologies will the data be stored and how will it be transmitted?
- In what geographic areas will the data be shared and/or stored?
- What are the known security and privacy vulnerabilities/risks?

IoT or OT devices must not be integrated into an Agency IT system unless approved by M/CIO after a Security Assessment and Authorization (SA&A) based on **NIST SP 800-213** controls has been completed, consistent with legal and policy requirements such as those outlined in **ADS 502**, **508**, **509**, and **545**.

547.3.6.2 Acquisition of IoT / OT Devices & IoT Waiver Process

Effective Date: 08/05/2024

The **Internet of Things Cybersecurity Improvement Act of 2020 (IoT Act)**, **OMB M-24-04**, **Federal Information Technology Acquisition Reform Act (FITARA)**, and **40 U.S.C. § 11319(C)(i)(I)** require that before an Agency may enter into a contract for IT or IT services, the Agency CIO must review and approve the contract.

Contracting Officers (COs) must ensure that M/CIO has reviewed and approved contracts that contain IT or IT services using IoT/OT devices via the M/CIO IT Authorization inbox (**ITAuthorization@usaid.gov**) prior to issuing a contract (see **ADS 302.3.5.12**). Planners must comply with the planning requirements in **ADS 300.3.5.4**, including conducting market research before requesting approval of an IoT device. Planners should review the **Approved Product Catalog** (accessible via the Agency intranet) for devices approved for Agency use as part of performing market research. CORs, System/Business Owners and/or ISSOs that identify a need to acquire IoT/OT devices that have not been identified in the contract must conduct market research/analysis of alternatives before requesting approval of an IoT device that is not currently approved for Agency use (see **Approved Product Catalog** and **ADS 509**).

Under the IoT Act, if M/CIO reviews a contract for an IoT/OT device, and determines during that review that using the device would prevent the Agency from complying with NIST's IoT standards and guidelines, then the Agency is prohibited from using the device, procuring or obtaining the device, or renewing a contract to procure or obtain the device.

The OU Planner, COR, Business/System Owner, Systems Manager, and/or ISSO should work with M/CIO Client Services to identify an alternate IoT solution. If the OU would like to obtain or procure the prohibited IoT/OT device, the OU must submit a formal prohibition waiver request to the CIO via **cyberrisk@usaid.gov**. The Agency CIO may waive the prohibition when at least one of the below conditions has been met:

1. The waiver is necessary in the interest of national security;
2. Procuring, obtaining, or using the IoT device is necessary for research purposes; or
3. The device is secured using alternative and effective methods appropriate to its function.

The Agency CIO must memorialize and justify any waiver recommendations in a signed

memorandum for the Administrator or their official designee. Upon receiving that memorandum, the Administrator or their designee may issue a waiver of the prohibition on use or acquisition of the device in question. The waiver must include the following, at a minimum:

1. Date of issuance;
2. The device(s) and any associated solutions or platforms covered;
3. A description of the purposes for which or the circumstances in which the device may be acquired or used;
4. The effective period of the waiver, which may not exceed two years;
5. A copy of the memorandum setting out the CIO's determination; and
6. The signature of the Administrator or their designee.

If a waiver is issued by the Administrator or their designee, the Agency CIO must make these waivers available to OMB's Office of the Federal CIO upon request. The CIO and the CO, COR, Business/System Owner, or System Manager must ensure that approved waivers are documented in relevant system security plans, and shared with acquisition officials for documentation in relevant contract files.

System Owners must also submit revised technical documentation to the Bureau for Management, Office of Management Services, Information and Records Division (M/MS/IRD) (see **502.3.4.2 Documentation for Electronic Systems**) for additional guidance.

547.3.7 Safeguarding IT Assets

Effective Date: 11/20/2019

The USAID workforce must take proper care of individually assigned Agency IT assets and ensure that they are used in accordance with Agency policies. Individuals and/or contractor companies may be held financially liable for all individually assigned property that is lost, damaged, or destroyed through improper use or willful action.

If USAID/W IT assets are damaged, missing, lost, or stolen, members of the USAID workforce (direct-hire employees, Personal Services Contractors, Fellows, Participating Agency Service Agreement, etc.) must immediately notify their supervisor, the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov**, and the AMS/EMT Officer. In USAID/W, the USAID workforce must also report the theft of government furnished equipment to local law enforcement and provide a copy of the police report to their supervisor and the M/CIO Service Desk.

When contractors notify the COR regarding damaged, missing, lost, or stolen IT assets,

the COR must notify the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** and the AMS/EMT for their organization (see **ADS 306mah** for additional guidance). The AMS/EMT or the CO must conduct an evaluation to determine liability.

When IT assets located at Missions are damaged, missing, lost, or stolen, overseas individuals must notify the EXO or System Manager and the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov**. In instances where government furnished equipment (IT assets) are stolen, the individual must also provide documentation to the EXO, System Manager, and the M/CIO Service Desk indicating that an official theft report has been filed with the Regional Security Office. Overseas contractors (institutional and PSCs) must follow the guidance in **547.3.5.2**. M/CIO will ensure that both USAID/W and Mission equipment is removed from the network.

If the AMS/EMT Officer or the EXO determines that the damage, loss, or theft was a result of the individual's actions, the individual may be required to pay the cost to repair or replace the property. M/CIO will provide the AMS/EMT Officer or EXO with an estimate of the depreciated replacement costs for lost or damaged IT assets and, upon receipt of the full amount of the funds from the B/IO or Mission, will replace the lost or damaged property.

When IT property is damaged, missing, lost, or stolen, the following procedures must be followed after the damage or loss is reported to the M/CIO Service Desk, AMS/EMT Officer, COR, and the EXO at all times:

1. USAID staff (U.S. Direct-Hires, Personal Services Contractors, Detailees, and PASA/RASA, etc.) must fill out an **AID 534-1, Personal Property Disposal Authorization and Report** and submit that form to the AMS Officer in USAID/W with a copy to M/CIO. For USAID/W, see **ADS 518, Personal Property Management (Domestic)**, for overseas locations, see **ADS 534, Personal Property Management Overseas** and **14 FAM 411**. The report must be filed within five days of discovering damaged, missing, lost, or stolen assets. The report must include complete details of the incident, a description of the equipment, barcode, serial numbers, and the name and telephone number of the person reporting the incident.

2. In USAID/W, after conducting the evaluation, the M/CIO Property Manager must provide a written notification to the AMS/EMT Officer or the COR of the outcome of the M/CIO technical evaluation and investigation as to the cause of the damage or loss of the IT asset. The AMS/EMT Officer or COR will determine, in consultation with the individual's supervisor, if the individual will be required to reimburse the government for the damaged, missing or stolen IT asset(s).

3. In Missions, after conducting the evaluation, the M/CIO Property Manager must provide a written notification to the EXO or SM of the outcome of the M/CIO technical evaluation and investigation as to cause of the damage to, or loss of,

the IT asset. The EXO, SM, or designee, in consultation with the individual's supervisor, will determine if the employee is required to reimburse the government for the damaged, missing, or stolen IT asset(s) and then advise the employee of the determination of liability.

4. For contractors, the COR must conduct an evaluation in coordination with the AMS/EMT Officer or EXO, and M/CIO. M/CIO will provide a technical evaluation and investigation of the missing, lost, stolen, or damaged equipment to include the estimated cost of equipment value/repair and notify the COR, CO, and the AMS/EMT Officer. The CO's final determination of liability will be made in accordance with the applicable property clause in the contract.

5. The M/CIO technical evaluation and investigation serve to:

- Relieve the AMS/EMT Officer or EXO of accountability for the asset;
- Provide the decision makers with a technical understanding of what happened to the IT asset; and
- Recommend corrective action for any disclosed internal control weakness.

6. If M/CIO is unable to locate the USAID/W IT assets after an investigation, M/CIO must enter the resource as missing or stolen in inventory records and remove the equipment from the inventory.

7. If capitalized property is determined to be missing, lost, stolen, or damaged, M/CIO must send a copy of the final **AID 534-1, Personal Property Disposal Authorization and Report** to M/CFO for adjustment to the General Ledger.

8. If IT assets are determined to be damaged, missing, lost, or stolen during the Separation and Exit Clearance Process (see **ADS 451, Separations and Exit Clearance**) in USAID/W, M/CIO must not approve clearance in Section 2: Administrative Clearances of AID 451-1, and must refer the matter to the B/IO AMS/EMT Officer with guidance regarding the technical evaluation and investigation of the damage to the equipment and the potential cause of the damage or loss, including whether it was the result of the normal wear and tear or carelessness or misconduct. M/CIO will provide the B/IO with a cost estimate on the cost of repair or replacement of the IT asset. Upon acceptance of the cost estimate by the B/IO point of contact (POC) with budgetary authority, M/CIO will assist the B/IO in repairing or replacing the IT property. The POCs for administrative clearances must determine when the individual is liable for the loss or damage of assets. All USAID property management regulations and any other U.S. Government laws and mandates apply. If the POC for administrative clearances determines that the loss or damage resulted from actions of the individual user, including user misconduct, the individual may be required to pay the cost of repair or replacement of the asset. The POC for administrative

clearances must inform the individual of any outstanding indebtedness and provide guidance on how to pay the debt prior to separation. The POC must enter the amount of unpaid debt in the designated section of the **AID 451-1** form. M/CIO and the B/IO AMS/EMT Officer must document the decision that the individual should be charged for repair or replacement on **AID 451-1**. M/CFO will collect any outstanding debt in accordance with the procedures outlined in **ADS 625, Accounts Receivable and Debt Collection**.

9. If IT assets are determined to be damaged, missing, lost, or stolen during the Separation and Exit Clearance Process in Missions, then the EXO must conduct an evaluation to determine if the damages are due to normal wear and tear or if they are due to actions of the individual user (see Section 2: Information Technology and Library Resources of **AID 451-1** and **ADS 451, Separations and Exit Clearance** for guidance). The EXO is responsible for collecting reimbursement from the individual for repair or replacement of the property if it is determined that the individual is liable for loss or damages by the EXO.

547.3.8 IT Hoteling (Guest) Workstations

Effective Date: 11/20/2019

B/IO/Ms may contact the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** to request assistance to designate either a permanent or floating guest computer. All permanent guest desk spaces must be approved by M/MS/HMD to ensure the space is accounted for in the Agency's space management and design plan.

For designated hoteling desk space, USAID approved users must login to the computer using their PIV or PIV-A card to access the USAID network. All hoteling IT assets must be assigned by M/CIO to the B/IO/M AMS or EXO. Only guests with USAID-issued credentials are authorized to use guest computers.

547.3.9 Opening, Moving and Closing a Mission

Effective Date: 11/20/2019

M/CIO maintains a wide area network (WAN) that provides overseas Missions and their users with access to the Agency's enterprise applications and IT assets. The WAN consists of systems that support network voice and data, security components, and server infrastructure, and it includes AIDNet and may include Guest Wireless. Given this, M/CIO must be involved in critical activities, such as when new Missions are established and when existing Missions relocate or close, because the Mission's core business is dependent upon a properly functioning IT infrastructure.

M/CIO is responsible for, and will perform installation and/or disposition of, IT services and assets when a Mission opens or closes. M/CIO is responsible for all IT procurement for the Mission, and the Mission must allocate adequate funds for the procurement of IT services or assets, as well as the installation or disposition of the IT services or assets. M/CIO provides planning, requirements gathering, design and engineering assistance

for phone systems that are procured by the Mission. Missions must perform acquisitions for phone systems (see **ADS 527maa** and **ADS 527mab**).

Missions must reimburse M/CIO for U.S. Direct-Hire travel that is required to maintain the AIDNet Authority to Operate. Additionally, Missions must compensate M/CIO for labor (project management, engineering, asset management, and deployment technicians), equipment (network, security, cabling, wireless, and servers), shipping, and travel costs (airline tickets, other transportation, per diem, and other approved fees) for openings, moves, and closures. There are some tasks that must be initiated and completed by Mission staff in order to open, move, or close a Mission; contact the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** for guidance. Tasks that can be accomplished by Mission personnel will be considered by M/CIO to reduce costs, but will require a risk assessment that is based on the availability of, and skillsets of Mission personnel. M/CIO may need to deploy staff to Missions for closures. When M/CIO does not need to deploy staff to assist in a Mission closure, M/CIO can provide guidance remotely, and Missions must cover disposal costs.

547.3.10 Secure Authentication Tokens

Effective Date: 08/05/2024

M/CIO maintains an inventory of Tokens (*e.g.,* soft and hard tokens) for remote and telework access. These tokens are assigned to the USAID workforce. Soft tokens that are not used within one year are subject to deactivation; individuals must reapply for a token in the event of deactivation (refer to **https://pages.usaid.gov/M/CIO/remote-access** for information on requesting a soft token). Hard tokens are considered PIV-Alternative credentials and are primarily issued to overseas staff who are Cooperating Country National (CCN) PSCs, Third Country National (TCN) PSCs, or Foreign Service Nationals (FSN). For these cases, eligible staff receive USAID PIV-A cards after meeting the requirements of a National Agency Check (NAC) (see **ADS 542**).

Individuals must obtain a signed waiver from their AMS in AID/W to request assignment of a hard token. If a hard token is lost, stolen, or broken, the individual must report this as soon as possible to the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov**. Individuals may be held financially liable for the replacement cost of hard tokens that are damaged or destroyed as a result of the individual's conduct.

547.3.11 Leased or Loaned Commercial Property

Effective Date: 11/20/2019

Loaning IT assets to the U.S. Government is not specifically prohibited by law, but is generally contrary to public policy. IT assets may only be leased or loaned to the Agency in USAID/W Operating Units and overseas Missions after M/CIO has reviewed the requirements and compared the need to available Agency assets or those of other agencies.

If M/CIO determines that requirements cannot be met internally or more cost effectively through acquisition, the property may be leased or loaned. When the EXO or B/IO leadership administratively determines that the lease or loan is clearly in the interest of the U.S. Government, M/CIO must approve and formalize the loan, setting forth the responsibilities of the government and the lender.

The B/IO AMS/EMT Officer must account for, and control, IT assets that are leased or loaned to USAID by the same standards as those applicable to USAID-owned property. Either the AMS/EMT Officer or M/CIO must issue a Form **OF-7, Property Pass**, as required, to the individual to authorize the removal of loaned property from an Agency-occupied building.

The loan of IT equipment cannot exceed 90 days. If a loan extension is requested, the same approval process is required.

547.3.12 Receipt and Inspection of IT Assets

Effective Date: 11/20/2019

Each Agency organization must apply the property management principles specified in this ADS chapter to OE-funded and program-funded contractor IT assets if the IT assets are acquired by USAID or purchased by contractors on behalf of USAID and installed in USAID space.

a. Upon receipt of equipment in AID/W M/CIO Asset Management must immediately inspect IT property and compare the shipment with the procurement documents and packing slip to ensure that acquisitions are in accordance with the required condition, quality, and quantity. M/CIO Asset Management must barcode and enter the received IT assets into the ITAM inventory system.

b. In Missions, Systems Managers must test equipment upon installation and immediately notify the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** of any equipment problems. All devices received overseas are previously barcoded. If the barcode is not on the device, the EXO or the System Manager must contact the M/CIO USAID Asset Management Group via the M/CIO Service Desk at M/CIO at (202) 712-1234 or **cio-helpdesk@usaid.gov** to obtain a barcode. Per **547.3.3.1**, IT assets must not be procured locally or in country.

547.3.13 Separation and Transfer Procedures for USAID/W and Missions

Effective Date: 11/20/2019

In accordance with the **Clinger-Cohen Act, FITARA**, **OMB M-16-02**, and **ADS 509, Management and Oversight of Agency Information Technology Resources**, the Chief Information Officer is responsible for the management of Agency IT assets, including the inventory and storage of those assets, to ensure that IT assets are effectively managed and safeguarded against waste, loss, and misuse.

547.3.13.1 USAID/Washington Separation or Transfer Procedure
Effective Date: 11/20/2019

Members of the USAID workforce must notify the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** ten business days in advance of their scheduled departure date. The M/CIO Service Desk will schedule an appointment to collect the IT asset(s) for inspection and/or sanitation (see **547.3.4.1** for additional guidance on assignment of IT assets). AMS Officers are not authorized to transfer IT assets to or between USAID/W individuals. The M/CIO IT assets assigned to an individual must be used by that individual when they transition to alternate assignments and the Supervisory AMS from the current B/IO must open a ticket with the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** to reassign the endpoint device to the new B/IO Supervisory AMS Officer.

See **547.3.7, Safeguarding IT Assets** for guidance on how to address missing, lost, stolen, or damaged IT assets during exit procedures.

547.3.13.2 Mission Separation or Transfer Procedure
Effective Date: 11/20/2019

The Mission EXO, or designee, must contact the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** 10 business days in advance of the scheduled departure of an individual to request an inventory of the IT assets assigned to the individual. The EXO must then provide an updated inventory of the IT assets that were collected from the departing individual to the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov**.

The EXO, or designee, must contact the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** at least 10 business days in advance of the individual's scheduled departure to request an inventory of IT assets assigned to the individual. The EXO must then provide the M/CIO Asset Management Group (via the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov**) with an updated inventory of the IT assets that were collected from the departing individual.

See **547.3.4.2** for additional guidance on assignment of IT assets. See **547.3.6, Safeguarding IT Assets** for guidance on how to address missing, lost, stolen, or damaged IT assets.

547.3.13.3 Institutional Contractors Separation or Transfer Procedure: Control of Information Technology (IT) Assets Provided as Government-Furnished Property (GFP)
Effective Date: 11/20/2019

USAID/Washington Procedure

The Contracting Officer's Representative (COR) must submit the IT assets to the

cognizant B/IO Administrative Management Staff (AMS) officer within two business days of contract expiration or the contractor's return of the IT assets, along with a written request that the asset be forwarded to M/CIO. The AMS Officer must coordinate the transfer of the IT asset(s) to the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** for inspection, sanitation, and/or redisposition. CORs and B/IO AMS officers are not authorized to hold IT assets indefinitely nor are they authorized to transfer IT assets to or between contractor employees or programs.

In instances where the contractor employee is assigned to a different USAID/W Bureau or Office as required under the contract (assuming the individual continues to perform services under the same contractual mechanism), the contractor employee may continue to utilize the security/authentication token (to include soft tokens) that was issued to the contractor employee. Soft tokens are apps that are stored on electronic devices, such as a laptop or mobile phone, and they may be installed on a personal device upon transfer. The use of a security/authentication token will enable the contractor employee to maintain his or her login credentials and email account, allowing the contractor employee to continue to work in a new location.

Mission Procedures

CORs in field Missions will coordinate with the EXO or CO, as designated by the Mission procedures when an institutional support contract expires or an IT asset is no longer required for contractor performance. At least ten business days in advance of the contractor's scheduled departure, the EXO must contact the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** to request an inventory of IT assets that are assigned to the contractor. The EXO must then provide the M/CIO Asset Management Group (M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov**) with an updated inventory of the IT assets that were collected from the departing contractor, and store the IT assets prior to reassignment. In the event that the contractor employee remains employed under the same contract but is assigned to a different Mission, the contractor employee may continue to utilize the security/authentication token issued to them.

See **547.3.7, Safeguarding IT Assets** for guidance on missing, damaged, or stolen IT assets.

547.3.14 Excess Capitalized Property

Effective Date: 11/20/2019

M/CIO must report all excess capitalized property in USAID/W or overseas to M/CFO, via a completed copy of Form **AID 534-1, Property Disposal Authorization and Report**, for adjustment to the General Ledger.

547.3.15 Decommissioning Hardware and Software

Effective Date: 11/20/2019

Proper decommissioning of OE and Program-Funded hardware and software is critical to maintaining the security of the USAID network. All IT assets and software must be approved for use on the network by M/CIO. When discovered, unapproved IT assets, software, or IT systems will be removed and the B/IO/M will be required to follow decommissioning guidance provided by M/CIO. For guidance on approved software contact M/CIO/IPM/ECM at **ecm@usaid.gov** and refer to the **M/CIO Services Page for approved hardware**, IT Standards & Guidance. USAID is committed to managing its IT assets in an organized, deliberative, and cost-effective manner.

When decommissioning as part of an Agency-wide technology refresh, rapid changes in technology and cybersecurity requirements necessitate the need for an Agency-wide systematic plan to upgrade and replace computers, peripherals, and other technologies to ensure that the Agency's network remains secure. In compliance with **Executive Order: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure**, M/CIO will work with B/IO/Ms to decommission IT assets and software based on the following factors:

- The age of the IT equipment;
- If the warranty is still active;
- The availability of upgrades and patches; and
- The status of vendor support.

M/CIO will work with B/IO/Ms once an OE or Program-Funded IT asset or software has been identified as being a candidate for decommissioning to determine replacements or upgrades as appropriate (see **547.3.16.2, Software Version Upgrade Requirements**, for additional guidance on decommissioning software).

547.3.16 Agency Software

547.3.16.1 Agency Software Inventory

Effective Date: 11/20/2019

In compliance with **Public Law No: 114-210 (MEGABYTE Act of 2016)** and **OMB M-16-12**, M/CIO manages the procurement of enterprise software licenses on behalf of the Agency. M/CIO must track software licenses purchased by USAID to ensure that the Agency is taking advantage of government-wide software license agreements and cost-reduction strategies, helping to reduce unnecessary duplication throughout the Agency. IT software includes the costs of commercial software licenses, subscriptions (including Software-as-a-Service (SaaS)), as defined in NIST Special Publication 800-145), and maintenance (upgrades, patches). B/IO/Ms are not authorized to purchase and/or install any software that is not approved for use by M/CIO (contact M/CIO/IPM/ECM at **ecm@usaid.gov** to request more information on software approved for use on the network. If a B/IO/M needs software that is not approved for Agency use, the B/IO/M

must submit a **software and hardware approval request (SHARP)** to M/CIO for consideration. The request must be approved through the SHARP process before M/CIO will approve the software acquisition request.

Missions connected to OpenNet must follow Department of State guidelines.

The USAID workforce must comply with copyright licenses for software items. The following accountability standards apply to USAID/W and USAID Missions that are connected to the USAID network (AIDNet).

1. Only software that is approved by M/CIO may be loaded onto USAID Government Furnished Equipment (GFE).

2. Installation of Software: Licensed software used for USAID business may only be used on USAID GFE. However, soft tokens (*e.g.,* RSA Soft Tokens) may be installed on non-GFE equipment. Software plug-ins used to enable remote access are not licensed and may only be downloaded onto personal equipment.

3. Approval Requirements: Prior to purchasing software approved for use on the network, B/IO/Ms must submit a ticket to the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** to request M/CIO approval to purchase the software license(s).

4. USAID Software Inventory: B/IO/Ms must report license information for any purchased approved software to the M/CIO Asset Management Group (via the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov**) within 30 days of purchase. This information goes into M/CIO's software license inventory and is used when the Agency negotiates terms with vendors enabling the Agency to reduce duplicative procurements and conduct trend analyses of Agency software use.

5. License Tracking: Missions must track license usage of any locally purchased approved software, and must submit that data to the M/CIO Asset Management team in order to ensure that it is accounted for in the Software License Inventory.

6. Internally developed software (*e.g.,* custom developed software): See **ADS 547maa** for guidance.

7. Capitalized COTS software: When a B/IO/M procures a site license or standalone software (*e.g.,* COTS) valued at the capitalization threshold of $25,000 or higher, it must report that software as capitalized property to the M/CIO Accountable Property Officer (see **ADS 629.3.2.2** for additional guidance).

8. Capitalized Internal Use Software: The capitalization threshold for internal use software defined as custom developed applications and/or software costs for appropriated fund accounts is $300,000 or above. Costs below that threshold

level must be expensed (see **ADS 629.3.6.1** for further guidance on capitalization for internal use software).

B/IO/Ms must ensure that, within 30 days of purchase of M/CIO approved software, they provide the M/CIO Asset Management Group (M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov**) the following information to support management of all Agency software (as required by **OMB M-16-12**):

- Manufacturer,
- Product description,
- Terms of Service,
- Number of licenses,
- Activation codes,
- Period of performance, and
- Purchase order number.

547.3.16.2 Software Version Upgrade Requirements

Effective Date: 11/20/2019

To keep the Agency network secure, USAID must ensure that software is up-to-date and patched; older software versions may have known security flaws that are corrected in newer versions and related patches.

To ensure that appropriate privacy and security controls are implemented, as well as to ensure compliance with Section 508 of the Rehabilitation Act, M/CIO requires that all IT software applications on GFE devices (*e.g.,* desktops, laptops, tablets, and cellular phones) be aligned to the Agency's Enterprise Architecture and must be maintained within two major versions of what the vendor is currently offering (*e.g.,* Adobe Acrobat Professional version x).

Users must not install operating system software updates on mobile phones, tablets, or laptops until M/CIO notifies the Agency that such updates have been tested and are approved for installation since updates may activate mobile location services or other capabilities not approved for use on the equipment.

M/CIO must oversee upgrades to all corporate applications. If a B/IO/M purchases software that is not part of the Agency's corporate offerings, then the B/IO/M must ensure that the procured version of the software meets M/CIO version requirements. For a list of approved software/versions, B/IO/Ms should contact M/CIO/IPM/ECM at **ecm@usaid.gov**. When a B/IO/M identifies a need to procure unapproved software,

they must submit a **SHARP request**. B/IO/Ms must not procure software that is not approved for use by M/CIO. M/CIO will remove unapproved, disapproved, and retired software from the network when identified. B/IO/Ms must ensure that ongoing maintenance costs for keeping the software up-to-date are incorporated into annual B/IO/Ms budgets. B/IO/Ms are responsible for procuring the software upgrades or patches for B/IO/M procured software, and must contact the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** to schedule installation of the updated version (see **ADS 549.3.3 Install, Move Add, and Changes** for additional guidance on installation). In instances where software upgrades have been discontinued by the vendor and vendor support is no longer available, the B/IO/M must work with M/CIO to identify viable software alternatives that meet the Agency's security, privacy, and 508 compliance requirements.

B/IO/Ms must ensure that, upon procurement of M/CIO approved software version upgrades, they provide the M/CIO Asset Management Group (via the M/CIO Service Desk, **cio-helpdesk@usaid.gov**) with software license information as outlined in **547.3.16.1**.

If a B/IO/M becomes aware of a newer version of B/IO/M procured software, the B/IO/M must notify M/CIO by contacting the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov**. When a newer version of software becomes available, M/CIO will notify all users of the older versions that the software must be upgraded. Once software has been upgraded, M/CIO will remove the older version from AIDNet and GFEs.

547.3.16.3 Software Disposition

Effective Date: 11/20/2019

When software is disposed of through redistribution, transfer, sale, grant-in-aid, or project contribution, or when donation seems merited, overseas Missions must follow the conditions of the licensing agreement regarding transfer of ownership.

When software is transferred, reassigned, exchanged, or sold to non-government organizations, the original documentation and media disks for the software must accompany it. The original owner of the software must execute proper license transfer documentation with the software manufacturer. In instances where no original documentation or disks are available or are outdated, the B/IO/M must provide online access to the account for these purposes.

IT software that is not transferred, reassigned, exchanged, or sold in accordance with licensing agreements must either be returned to the licensor or destroyed if the Property Disposal Officer (PDO) determines in writing that destruction is the most cost-effective disposal approach. The PDO must ensure that property records are updated to reflect the manner of disposition.

547.4 MANDATORY REFERENCES

547.4.1 External Mandatory References
Effective Date: 08/05/2024

a. 14 FAM 411

b. 15 FAM 100

c. Clinger-Cohen Act of 1996

d. Federal Acquisition Regulation (FAR), Part 1, Subpart 1.3, Agency Acquisition Regulations

e. Internet of Things Cybersecurity Improvement Act of 2020 (IoT Act)

f. MEGABYTE Act of 2016

g. OMB Circular A-130

h. OMB M-16-02

i. OMB M-24-04, Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements

j. National Institute of Standards & Technology (NIST) Special Publication 800-213 Series

k. NIST SP 800-82, Guide to Operational Technology (OT) Security

l. Title VIII, Subtitle D of the National Defense Authorization Act (NDAA) for Fiscal Year 2015, Pub. L. No. 113-291 (Federal Information Technology Acquisition Reform Act (FITARA)

547.4.2 Internal Mandatory References
Effective Date: 01/11/2024

a. ADS 302, USAID Direct Contracting

b. ADS 405, Telework and Remote Work Program

c. ADS 451, Separations and Exit Clearance

d. ADS 518, Personal Property Management (Domestic)

e. ADS 527, Functions of the Mission Executive Officer

f. ADS 527mab, Administrative Guidance on How to Close a USAID Operating Unit - Checklists

g. ADS 534, Personal Property Management Overseas

h. ADS 549, Telecommunications Management

i. ADS 625, Accounts Receivable and Debt Collection

j. ADS 629, Accounting for USAID-Owned Property and Internal Use Software

547.4.3 Mandatory Forms
Effective Date: 11/20/2019

a. AID 534-1, Personal Property Disposal Authorization and Report

b. AID 547-1, Business Waiver Request For Additional Government Furnished Equipment (GFE) Outside Standard Equipment Package

c. OF-7, Property Pass

547.5 ADDITIONAL HELP
Effective Date: 11/20/2019

There are no Additional Help documents for this chapter.

547.6 DEFINITIONS
Effective Date: 08/05/2024

See the ADS Glossary for all ADS terms and definitions.

Accountable Property
Accountable property for USAID is (a) all nonexpendable residential furniture and equipment regardless of cost or location; (b) all other nonexpendable personal property items costing $200 or more, exclusive of shipping, packing and storage costs; (c) any expendable stock inventory in stockroom or nonexpendable property in warehouse; and (d) any leased or borrowed nonexpendable property regardless of cost. (**Chapter 534** and **547**)

Accountable Property Officer (APO)
Official(s) appointed by Agency Property Management Officers (*e.g.,* EXO or AMS/EMT Officers serve in this capacity) who are responsible for IT property. The official who is charged with budgeting, accountability, receipt, storage, issuance, record keeping, inventory, reporting, and certification of all Federal Information Processing (FIP) resources records and reports within the accountable area. (**Chapter 532** and **547**)

Acquisition Manager
The designated official who is responsible for procuring IT services and supplies with appropriated funds. (**Chapter 547**)

Agency Organizations
In USAID/Washington this includes Bureaus and Independent Offices. Overseas this includes USAID Missions, USAID Offices, USAID Sections of Embassy, Offices for Multi-country Programs, Offices for Multi-country Services, etc. (**Chapter 541** and **547**)

Application Software
A program or group of programs designed for end users. These programs are divided into two classes: system software and application software. While system software consists of low-level programs that interact with computers at a basic level, application software resides above system software and includes database programs, word processors, spreadsheets, etc. Application software may be grouped along with system software or published alone. Application software may simply be referred to as an application. (**Chapter 547**)

Capitalized Personal Property
Capitalized personal property is nonexpendable personal property that has an invoice cost of $25,000 or more and an estimated service life of two years or longer that must be capitalized and reported on in the Agency's financial statements. State vehicles are capitalized property regardless of cost. For USAID, vehicles with a basis acquisition cost of under $25,000, including shipping costs, are not capitalized. (**Chapter 534** and **547**)

Commercial Property
Property that is available through lease or purchase in the commercial market. (**Chapter 547**)

Endpoint Device
Computing device that communicates back and forth with a network to which it is connected. Examples of endpoint devices include: desktop computers, laptops, workstations, smartphones, tablets, and servers. (**Chapter 547**)

Enterprise Infrastructure Software
Provides capabilities required to support enterprise software systems. (**Chapter 547**)

Enterprise Software
Addresses an organization's needs and data flow in a huge distributed environment. (**Chapter 547**)

Excess Property
Property under control of a Federal agency, which is no longer required by the Agency for its needs. (**Chapter 547**)

Firmware
A semi-permanent software running on a system. (**Chapter 547**)

Information Technology
a. Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the Agency; where

b. Such services or equipment are 'used by an agency' if used by the agency directly or if used by a contractor under a contract with the agency that requires either use of the services or equipment or requires use of the services or equipment to a significant extent in the performance of a service or the furnishing of a product.

c. The term "information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including provisioned services such as cloud computing and support services that support any point of the lifecycle of the equipment or service), and related resources.

d. The term "information technology" does not include any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment. (Source: Clinger-Cohen Act, OMB M-15-14) (**Chapters 300**, **541**, **545**, **547**, **552**)

Information Technology Asset Management (ITAM)
The industry term for the application or suite of applications that track an organization's IT assets such as laptops, desktops, and mobile devices' assignment and life cycle. It usually involves gathering detailed hardware and software inventory information which is then used to make decisions about hardware and software purchases and redistribution. IT asset management helps organizations manage their systems more effectively and saves time and money by avoiding unnecessary asset purchases and promoting the harvesting of existing resources. Organizations that develop and maintain an effective IT asset management program further minimize the incremental risks and related costs of advancing IT portfolio infrastructure projects based on old, incomplete and/or less accurate information. (**Chapter 547**)

Open Source Software (OSS)
Software that can be accessed, used, modified, and shared by anyone. OSS is often distributed under licenses that comply with the definition of "Open Source" provided by the Open Source Initiative (**https://opensource.org/osd**) and/or that meet the definition of "Free Software" provided by the Free Software Foundation (**https://www.gnu.org/philosophy/free-sw.html**). (**Chapter 547**)

Operational Technology (OT)

Operational Technology (OT), defined by NIST SP 800-37 rev. 2 as "[p]rogrammable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms. (**Chapter 547**)

Property Custodian
The official responsible for day-to-day oversight, control, and safeguarding of IT property in USAID. (**Chapter 547**)

Property Disposal Officer (PDO)
The official designated in writing by the Property Management Officer (PMO). The Property Disposal Officer must not be the Accountable Property Officer (APO) in order to minimize the vulnerability of property to fraud or abuse. (**Chapter 547**)

Property Management Officer (PMO)
The overseas official (EXO or principal official), who is responsible for all Nonexpendable Personal Property (NXP) management functions. The official responsible for all personal property management functions including establishing internal policies and procedures for management and control of assigned personal property, ensuring implementation of such policies and procedures, and compliance with Agency and government-wide authorities and guidelines. (**Chapter 547**)

Proprietary Software
Software with intellectual property rights that are retained exclusively by a rights holder (*e.g.,* an individual or a company). (**Chapter 547**)

Restricted Space
An area where storage, processing, discussions, and handling of classified documents is authorized. (**Chapters 517, 547**, 552, 565, 567, 568)

Software
Programs, procedures, rules, and related data and documentation that direct the use and operation of ICT and instruct it to perform a given task or function. Software includes, but is not limited to, applications, non-web software, and platform software. The set of user programs running on a system that are designed to be updated often. (**Chapter 547, 551**)

Software as a Service (SaaS)
The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a Web browser (*e.g.,* Web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual

application capabilities, with the possible exception of limited user specific application configuration settings (NIST SP 800-145). (**Chapter 547**)

Source Code
Computer commands written in a computer programming language that is meant to be read by people. Generally, source code is a higher level representation of computer commands as they are written by people and, therefore, must be assembled or compiled before a computer can execute the code as a program. (**Chapter 547**)

USAID IT Investments
IT initiatives or projects funded at Missions or USAID/W, regardless of funding source, which are owned, licensed, or leased by USAID and operated by USAID or by contractors for Agency operations. (**Chapter 547**)

Workforce
"Workforce" and “Individuals” refers to individuals working for, or on behalf of, the Agency, regardless of hiring or contracting mechanism, who have physical and/or logical access to USAID facilities and information systems. This includes, but is not limited to United States Direct-Hire employees, Personal Services Contractors, Fellows, Participating Agency Service Agreement, and Contractor Personnel. Contractors are not normally subject to Agency policy and procedures as discussed in **ADS 501.1**. However, contractor personnel are included here by virtue of the applicable clauses in the contract related to information security requirements. (**Chapter 547**)

547_080524