ADS Chapter 549

Telecommunications Management

Partial Revision Date: 04/12/2021
Responsible Office: M/CIO/ITO
File Name: 549_041221

Functional Series 500 – Management Services
ADS 549 – Telecommunications Management
POC for ADS 549: Brian Herson, (202) 916-4640, bherson@usaid.gov

Table Of Contents

ADS Chapter 549 - Telecommunications Management

549.1 OVERVIEW

Effective Date: 12/15/2015

This chapter addresses the overall framework of telecommunications services including voice, video and data available within USAID. Telecommunications services refer to any technology, service, system, or other resource that provides or ensures transmission of electronic data, voice and/or information. Telecommunications resources may be voice and data networks, telephones (wired and wireless), other wireless services, messaging and directory services, high speed data communications, facsimile devices, personal digital assistants, network servers, switches, or any other device, service, or system used in the transmission of electronic communication, including the connectivity to and between devices. The locations of telecommunications resources are equally diverse, ranging from equipment in single buildings to nationwide or global networks to communications satellites.

Telecommunications services that are either all or part of a system must be considered as information technology (IT) components for all planning, acquisition, policy, security, and functional purposes.

549.2 PRIMARY RESPONSIBILITIES

Effective Date: 12/15/2015

a. The **Office of the Executive Secretary (ES)** must clear any Administrator or Acting Administrator signed telegrams including Agency Worldwide telegrams (AWIDE) signed by them.

b. The **Bureau for Management, Office of the Chief Information Officer (M/CIO)** manages the USAID/Washington (USAID/W) voice telecommunications network, services, equipment, and funding; data telecommunications in USAID/W, including guidance and oversight to the Missions; email in USAID/W and overseas; telecommunications services involving coordination of telegram regulations with other government agencies; preparation and distribution of all Agency telegrams; and maintaining hardware and software to support the Agency's telegram system. M/CIO is responsible for monitoring network activities, documenting and logging connectivity, measuring performance, taking corrective action to maintain operational status, and recommending and implementing network enhancements. M/CIO also provides guidance and assistance in establishing a reliable, consistent, and cost-effective telecommunications network for all overseas locations worldwide; connectivity to the Agency's network (AIDNET); and the ability to exchange information with other overseas locations, USAID/W, and external organizations (Private Voluntary Organizations (PVOs), contractors, vendors, universities, and other government and non-government organizations).

c. **Mission Directors** are responsible for Mission voice telecommunications including acquisition that is consistent with published M/CIO IT standards.

549.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

549.3.1 Telecommunications Management

Effective Date: 12/15/2015

Telecommunications equipment, facilities, and services will be used for conducting official government business. Limited personal use of USAID telephones, email and Internet services must not interfere with official duties, inhibit the security of information and information systems, or cause degradation of network services (see **ADS 545mam, Acceptable Use Policy for Information Technology Resources** and **ADS 545mbg, Wireless Standards and Guidelines**).

Telecommunications services will be provided to employees only when their jobs require such service to conduct official business.

549.3.1.1 Telecommunications Inventory

Effective Date: 05/11/2017

The Bureau for Management, Office of the Chief Information Officer (M/CIO), must maintain an inventory of telecommunications equipment. For the purposes of this chapter, telecommunications equipment includes, but is not limited to: computers (GFE laptops and desktops), VoIP phones (desk lines), computer monitors, mobile phones, tablets, printers, scanners, fax machines, infrastructure equipment (router, switch, hub, server, firewall, encrypter), RSA tokens, audio conferencing service accounts, and portable storage devices.

Due to the high cost of providing telecommunications equipment and services, M/CIO will periodically request that Bureau and Independent Office (B/IO) Administrative Management Staff (AMS) validate an inventory of telecommunications equipment assigned to the B/IOs to the M/CIO Property Management Officer.

549.3.2 Telegram Use and Preparation

Effective Date: 12/15/2015

Telegrams are one of the methods used to transmit USAID official business information. USAID employees must follow the policy and required procedures in section **549.3.2** through section **549.3.2.8** when establishing internal controls for telegram usage, approval, and clearance.

Routine cables are pro forma announcements of routine business decisions and actions. This includes personnel actions (assignments or reassignments, applications for benefits, separation cables, rest and recuperation, individual separation maintenance allowance, extension of tours, home leaves or transfers, medical clearance, security clearance, etc.), administrative finances (administrative audits, contracting support, U.S. or local payroll, administrative purchasing, etc.), and humanitarian disaster efforts (disaster declarations, disaster response, funding

transfers, etc.). Routine cables can be labeled (or "captioned" in cable parlance) ADM AID or AID HR Channel.

Substantive cables include communications of guidance that impact policy and budgetary decisions, have cross-cutting Agency implications beyond a single Bureau, or are related to priority initiatives. Substantive cables are usually captioned AIDAC.

The M/CIO USAID Cable Room manages the process for transmitting routine cables to the Department of State; while the USAID Office of the Executive Secretary (AID/ES) manages the process for substantive cables.

Please email **cable-terminal@usaid.gov** for guidance on procedures and instructions for transmitting routine telegrams via email.

549.3.2.1 Department of State (DOS) Standards for Telegrams

Effective Date: 12/15/2015

All Agency telegrams must comply with standards and procedures set by the Department of State's Inter-Agency Affairs Staff (DOS/IM/SO). Request for waiver or non-compliance must be pre-approved by DOS.

The Agency utilizes the Department of State's (DOS) international communication methods for transmission. Therefore, all Agency telegram preparations must conform to DOS rules and regulations. USAID/W offices must adhere to rules and procedures established by the DOS Communications Office.

The regional Bureaus have established collectives from their respective regions for transmitting outgoing telegrams to Agency Missions grouped by area. USAID/W collectives are: AID Worldwide (AWIDE), all African Posts (AIDAF), all Asia and Near East Posts (AIDAN), all European Posts (AIDEU), all Latin American and Caribbean Posts (AIDLA) and all AID Controllers (AIDCO). Please email: **cable-terminal@usaid.gov** for guidance on procedures and instructions for transmitting routine telegrams via email.

All outgoing Agency telegrams must begin with one of three captions: AIDAC, ADM AID, and AID HR Channel. These serve as an indicator for an administrative or project-related telegram and ensure proper dissemination and identification in USAID/W and USAID/Missions through DOS facilities.

549.3.2.2 M/CIO/IA Telegram Template

Effective Date: 12/15/2015

The M/CIO telegram template (which can be accessed via USAID's intranet at **https://pages.usaid.gov/M/CIO/classified-support-web-site**) must be used when preparing unclassified telegrams. For more guidance on telegrams or specific guidance on how to send and receive telegrams please email: **cable-terminal@usaid.gov**.

549.3.2.3 Telegram Clearance and Approval

Effective Date: 12/15/2015

All telegrams must be cleared and approved per the Agency's processes. For additional guidance on telegram clearance and approval please email: **cable-terminal@usaid.gov**.

The following are Agency officers who are authorized to approve telegrams or who have been delegated to do so:

- The Administrator (A/AID);
- Deputy Administrator (DA/AID);
- Executive Secretary (ES);
- Assistant Administrators (AAs);
- Deputy Assistant Administrators (DAAs);
- General Counsel (GC);
- Inspector General (IG);
- Office Directors reporting to the Administrator;
- Mission Directors;
- Mission Representatives; and
- Employees or officials acting in these positions**.**

549.3.2.4 Mission Approval Controls

Effective Date: 12/15/2015

Missions must implement appropriate procedures to provide effective controls over the dispatch of official telegrams at Mission locations. Only the A/AID, DA/AID, Assistant Administrators (AAs), and DAAs for each Bureau/Office are authorized to approve messages concerning major policy issues with regard to the objectives or conduct of the Foreign Assistance Program. They are also the only officials authorized to reverse a policy decision made by themselves or Missions.

549.3.2.5 Security Classification

Effective Date: 12/15/2015

All telegrams must be assigned a security classification, an administrative control designation, or be marked "UNCLASSIFIED" as appropriate.

Precedence designators must be used to prescribe the relative urgency for handling and transmitting telegrams.

Telegrams to overseas locations designated “MINIMIZE” must be transmitted only after an official authorized by the respective geographical Bureau determines that the message is urgent and essential.

549.3.2.6 Telegram Controls (Declassifying/Downgrading)

Effective Date: 12/15/2015

Every document containing a security classification must contain a notation outlining automatic, time-phased downgrading and declassification procedures for the document. As outlined in **12 FAM 540**, all Sensitive but Unclassified (SBU) telegrams must be sent “UNCLASSIFIED” with the distribution caption "SENSITIVE." The “SENSITIVE” caption must immediately follow channel captions (if applied). These telegrams must be transmitted via encrypted means over both unclassified and classified circuits (see **12 FAM 540**).

549.3.2.7 Telegram Distribution

Effective Date: 12/15/2015

The SMART Client was developed so that drafting messages would be fast, easy and intuitive to users. The SMART Client’s working email window looks similar to a normal Outlook email, with the exception that SMART classification, sensitivity, and preview/print functions are included. To access SMART Client on the unclassified side, users must contact the Department of State at (202) 712-2000 or via email at **ITServiceCenter@state.gov** to gain access via Opennet. For access to the classified SMART Client, the user must have a classified account. Please email **cable-terminal@usaid.gov** for further guidance and assistance.

549.3.2.8 Retention of Agency Telegrams as Official Agency Correspondence

Effective Date: 12/15/2015

Drafters and recipients of telegrams must retain final copies with approvals in official office or project files. Retention period guidance is found in **ADS 502, The USAID Records Management Program**.

549.3.3 Install, Move, Addition, Changes

Effective Date: 12/15/2015

M/CIO performs user IT installations, moves, additions and changes (IMAC) across USAID/W. Each IMAC of USAID/W IT assets must be performed by M/CIO personnel. B/IO AMS Officers must submit an IMAC request to the M/CIO Service Desk (**cio-**

helpdesk@usaid.gov) 10 business days in advance of the requested move or installation date (this includes setup and breakdown for conferences or large meetings).

For 10 or more IMACs over a 30-day period, M/CIO will provide the B/IO AMS Officer or designated budgetary authority point of contact, with a cost estimate of the funds required from the B/IO to complete the requested IMAC. Upon acceptance of the cost estimate by the B/IO point of contact with budgetary authority, M/CIO will schedule the action start date in coordination with the USAID/W requester.

549.3.4 Telephone Systems

549.3.4.1 Procurement, Installation, and Repair of Telephone Systems

Effective Date: 05/11/2017

M/CIO coordinates requests for telephone systems or required actions with the appropriate B/IO AMS Officer per the Federal Property Management Regulation (FPMR).

Malfunctioning telephones within the USAID/W telephone network must be reported to the M/CIO Service Desk (**cio-helpdesk@usaid.gov**). Changes in service must be requested through the organization's AMS Officer via a Service Desk request ticket.

Any organization relocating groups of employees must have the appropriate AMS and M/MS/HMD officials coordinate with M/CIO on funding transfer, telephone, wiring and computer issues. All coordination must be done prior to setting a move date. Telephones must only be moved by M/CIO technicians.

Requests for specialized telephone equipment or services must be submitted to M/CIO. Examples of specialized equipment or services include, but are not limited to:

- Standalone fax machines;
- Cellular phones/devices;
- Special equipment, non-standard, and hearing impaired: Requests for specialized telephone equipment or services not listed as standard offerings from vendors must also be submitted to M/CIO. Special telecommunications equipment for employees with impaired hearing must be provided;
- Voice mail: The Agency's standard voice network is rated only for transmission of unclassified information; and
- Audio conference service.

Malfunctioning telephones within the USAID/W telephone network must be reported to the M/CIO Service Desk (**cio-helpdesk@usaid.gov**).

549.3.4.2 Telephone Usage
Effective Date: 12/15/2015

Use of the government's telephone system is provided to conduct official business. Limited personal use of USAID telephones must not interfere with official duties, inhibit the security of information and information systems, or cause degradation of services (see **ADS 545, Information Systems Security** for additional guidance). Unofficial calls must not adversely affect the organization or the employee's performance of official duties.

549.3.4.3 Collect Calls
Effective Date: 12/15/2015

Collect calls must not be accepted at the expense of the government. Calls placed from one telephone to another but charged to a third Agency telephone number are not authorized.

549.3.4.4 Long-Distance Calls
Effective Date: 05/11/2017

Senior management officials of the Agency must ensure that long-distance charges are incurred only when required in support of official business.

Circumstances sometimes require employees to place long-distance calls to conduct Agency business from outside the office (*e.g.,* calling overseas locations with vastly different time zones). Toll calls placed from the employee's home must be completed in the most economical manner available. Reimbursement of each call must receive approval from the employee's immediate supervisor. Requests for reimbursement must be sent to M/CFO/CMP or the cognizant controller's office.

All outgoing telephone services from the domestic telephone systems (including local and long-distance) must be accessed by dialing nine. The telephone system automatically routes the call to the appropriate vendor for local, domestic long-distance, or international long-distance service. When practical, employees must make international calls when the rates are lowest.

Long-distance calling cards will no longer be issued to USAID/W staff. Current long-distance calling cards were deactivated effective October 31, 2016. Staff who need to make or receive government calls while away from their office may request a USAID cell phone from their AMS Officer (see **549.3.4.10**).

549.3.4.5 Audio Conference Service
Effective Date: 05/11/2017

Audio Teleconference Service accounts will only be issued by M/CIO to individual USAID/W Direct-Hire employees stationed in the United States for their use or the

use of their support staff to facilitate audio conference calls to conduct official business.

Direct-Hire staff may order accounts by completing and submitting the **AID 549-2 form** to the M/CIO Service Desk at **cio-helpdesk@usaid.gov**. Requests for an account must be approved by the employee's supervisor and AMS Officer.

Employees issued Audio Conference Service accounts accept responsibility for all calls made from the account and must protect the account from misuse. The requesting B/IO must notify the M/CIO Help Desk if the employee leaves that B/IO or if the account is no longer needed. If the account number is compromised, the employee or B/IO must notify the M/CIO Help Desk at **cio-helpdesk@usaid.gov**, or (202) 712-1234 immediately. Periodically, account holders may be required to review usage to verify if all calls were made by them, and the accuracy of the billing data, such as date, duration, and the number of participants.

549.3.4.6 Toll-Free Telephone Services

Effective Date: 12/15/2015

Requests for toll-free telephone services at Agency sites must be justified and submitted to M/CIO by the AMS Officer. The justification must explain why it is in the Agency's interest to provide this service.

549.3.4.7 International Telephone Calls

Effective Date: 12/15/2015

The M/CIO recommended options for placing international calls are:

- Department of State's International Voice (IVG) Gateway; and
- USAID Voice over Internet Protocol (VoIP).

Calls using IVG and USAID VoIP are limited to the Embassy or Mission's phone system, so callers can't call elsewhere in the country. Missions may use these networks to call anywhere in the U.S.

The **USAID staff directory** also has a link to the Post Call Forwarding List. This list enables USAID staff to call a phone number in the Ronald Reagan Building that is forwarded to an Embassy/Mission main phone line, which can then be forwarded to the appropriate extension.

Each Mission must fund their telephone systems and can select their telephone and long-distance service providers.

549.3.4.8 Listening-In/Recording Telephone Conversations

Effective Date: 12/15/2015

Under limited circumstances, USAID is authorized to listen-in or record telephone conversations per section 101-35.202 of the FPMR.

549.3.4.9 Fax Machines

Effective Date: 12/15/2015

Fax machines must be provided by M/CIO to Agency organizations to facilitate official government communication and must adhere to records management rules outlined in **ADS 502, The USAID Records Management Program**.

Fax machines will be issued in the most economical manner to the government. This includes issuing only the number of machines that are sufficient to accommodate the business function. In most cases, one machine will accommodate several offices or may be issued one per floor, site, etc.

Unless otherwise marked or designated, the Agency's standard fax network must be used only for the transmission of unclassified information.

Malfunctioning fax machines must be reported to M/CIO by contacting the M/CIO Service Desk at (**cio-helpdesk@usaid.gov**).

549.3.4.10 Mobile Phones

Effective Date: 07/09/2020

Mobile phones are available to be issued to Agency staff to facilitate conducting official business when approved by B/IO leadership or Mission EXOs. M/CIO recommends that mobile phones only be issued to staff who are required to travel or have an identified business need. M/CIO will maintain an inventory of mobile IT assets and associated service plans; B/IOs and Missions are required to validate this inventory annually or upon the departure of USAID/W and Mission staff (see **Information Technology Asset Management - Employee Separation and Transfer Procedures Agency Notice** for guidance on inspection, sanitation, redisposition and/or storage of mobile phones).

Members of the Agency workforce who are issued mobile phones must sign an agreement form outlining responsibility for the mobile phone and return the form to the AMS Officer or Mission Executive Officer. Members of the Agency workforce must forward a complete copy of an Agency record that is created using a mobile application (such as text messages, videos, recordings, documents, or notes) and stored only on an Agency-issued mobile phones to their official USAID email address (see **ADS Chapter 502, sections 502.3.4.7 Electronic Messaging and 502.3.4.8 Additional Standard for Text Messages on Government Furnish Mobile Devices**). The requesting organization AMS Officer must notify M/CIO if the employee leaves the organization or if the mobile phone is no longer needed. B/IO AMS Officers and Mission Executive Officers are responsible for selecting and controlling the voice and data plan for each employee. USAID/W AMS Officers are responsible for ensuring funds are made available to M/CIO to pay monthly service and overage charges.

Mobile device service plans with outstanding balances are subject to cancellation at M/CIO's discretion. M/CIO is responsible for reporting Bureau overage and zero usage reports on a monthly basis to the B/IO AMS Officers. Missions are responsible for paying monthly service and overage charges to their service provider.

Members of the Agency workforce must report damaged, missing, or stolen, mobile phones to: M/CIO Service Desk (**cio-helpdesk@usaid.gov**), their supervisor, AMS Officer or the Accountable Property Officer for their organization; contractors must notify their Contracting Officer's Representative (COR) who is responsible for reporting the damage or loss to their B/IO AMS Officer or Accountable Property Officer immediately.

Mobile phones that are assigned to an individual must be turned on, and must be connected to a data network (WiFi and/or Cellular Network), every 30 calendar days to ensure that approved updates (e.g., security patches) are installed to protect the Agency's devices (this may take two to six hours for users in the field depending on the WiFi or Cellular speed). When users do not turn on and connect their devices to a data network every 30 days, M/CIO will notify the user of intent to suspend the mobile account. If the user has not connected their device to a data network by the 31st day, M/CIO will suspend the account. On the 31st day, M/CIO will send a notification to the AMS Officers for Continental United States (CONUS) users and the SM/EXO for Outside the Continental United States (OCONUS) users that a user's account has been suspended and will be wiped if no action has been taken by the user on the suspended account within the next 60 calendar days. Upon receipt of the notification from M/CIO, AMS Officers and SM/EXOs should notify M/CIO if the device should not be wiped, based on the user being unavailable (such as on TDY, home leave, extended absence, etc). Under no circumstances should AMS Officers or SM/EXOs provide M/CIO with details as to the reasons underlying the employee's absence, however, information regarding geographic location is appropriate to share. On the 31st day, M/CIO will also notify the Office of the General Counsel (GC), the Office of Security (SEC), the Office of the Inspector General (OIG) (see **ADS 158**), the Records Officer (see **ADS 502**), the Office of Civil Rights and Diversity (OCRD), and the Office of Human Capital and Talent Management, Employee and Labor Relations Division (HCTM/ELR) of the account suspension and the intent to wipe the mobile phones after the 90th calendar day if the user has not connected to a data network.

If there is a pending litigation matter, investigation, or other requirement to maintain the data on the device, within the 60-day review window, GC, SEC, OIG, the Records Officer, OCRD, and HCTM/ELR must provide a written response to CIO that the device must not be wiped. In instances where GC, SEC, OIG, the Records Officer, OCRD, or HCTM/ELR require additional time to review, they must submit a written extension request to M/CIO in order for M/CIO to grant the additional time. M/CIO will move forward on wiping the mobile phone after the 90th day, absent receipt of a written response or a request for extension. The data stored on the devices will not be recoverable once the phones are wiped after the 90th day.

549.3.4.11 Mobile Device Operating System Updates

Effective Date: 02/10/2021

Mobile device users (*e.g.,* phones and tablets) must download Agency-approved updates to operating systems within 30 calendar days of the M/CIO Service Desk Notice announcement. M/CIO will suspend the mobile device account if the user fails to update the operating system. Prior to initiating the update, users should follow these steps for GFE mobile devices:

1. Charge the device to full battery capacity or keep the device plugged in during installation.

2. Ensure the phone is connected to a Wi-Fi network to download the iOS.

3. Select Settings > General > Software Update > Download and Install – iOS XX.X (the version will change). You may be prompted to make space if there is not enough storage for the update. If this occurs, follow these **instructions**.

4. Enter your device's unlock passcode when prompted.

5. Follow any unique instructions provided by Apple during your installation process, including terms and conditions agreement.

Users must ensure that they disable features that are highlighted in the M/CIO Service Desk Notice (*e.g.,* Location Services – OFF (All iPhones and iPads)). Please contact the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** for assistance in updating and managing your USAID provided mobile device.

549.3.4.12 Telephone Directories

Effective Date: 12/15/2015

M/CIO manages the USAID telephone directory, which is included in the Agency's Active Directory. M/CIO also serves as the Agency's coordinator with DOS for Agency input in DOS's Telephone Directory.

Changes and discrepancies with a staff members' contact information must be forwarded to the M/CIO Service Desk (**cio-helpdesk@usaid.gov**) for correction. B/IO AMS Officers are responsible for ensuring the accuracy of staff members' information.

549.3.4.13 Overseas Voice Telecommunications

Effective Date: 12/15/2015

The Agency's overseas organizations must comply with Agency guidance in order to provide the appropriate safeguards for U.S. Government information.

Each Mission has the authority to establish its own policies and procedures that align to USAID and Regional Security Officer policy, guidance, and directives for use of its telephone system per Agency telecommunication management policy (see **ADS 527,**

Functions of the Mission Executive Officer (Section 527.3.5) for additional guidance on interpretation and clarification of approved policies and procedures at posts abroad).

Overseas locations that need to upgrade or replace all or part of Agency-installed telephone equipment must coordinate with the DOS Regional Information Management Center (RIMC) for their Mission. The RIMC provides a variety of technical services to help manage the telephone system.

RIMCs assist with the selection of a system and equipment best suited for overseas requirements, environment, and connectivity with host country and embassy systems. M/CIO is also available for consultation.

Upon receipt of the RIMC's recommendations, overseas locations procure telephone equipment by:

- Ordering directly from vendors by using a purchase order; and
- Requesting the RIMC to order the equipment by providing them with appropriate fiscal data.

549.3.5 Data Telecommunications (AIDNET)

Effective Date: 12/15/2015

Access to the Agency's data communications network will be granted to personnel who have:

- The appropriate background check or a security clearance commensurate with the highest classification of information ever processed or stored on the system;
- Once a Personal Identity Verification (PIV or PIV-A) card or a two-factor logical access card is granted, individuals may be approved for network access;
- Appropriate access levels and need-to-know in connection with the performance of official duties; and
- Knowledge of their computer security responsibilities (see **ADS 545, Information Systems Security**).

Individuals with authorized access to the Agency's data communications network must complete the Agency's Computer System Access Request Form. Contact the M/CIO Service Desk (**cio-helpdesk@usaid.gov**) or the B/IO/M AMS Support Officials to obtain this form.

549.3.5.1 Remote Access

Effective Date: 07/17/2017

The USAID remote access Internet domain name is considered SBU information and Agency information must not be published, distributed, or written where it is easily obtained by unauthorized individuals.

Remote access must occur only through M/CIO provided solutions. All software and hardware used for remote access activities must be approved by M/CIO. Please contact the M/CIO Service Desk (**cio-helpdesk@usaid.gov**) or refer to **ADS 545, Information Systems Security** for additional guidance.

Individuals accessing any of the Agency's computer systems from an unsecured site, (*i.e.,* their home or business office, or another government site) must safeguard their access media and login through M/CIO sanctioned sites using either a hard or soft RSA remote access token that has been issued to the user by USAID. Please see **ADS 545** for additional guidance. Accessing applications through SBC or VDI protects the Agency against potential data loss and information spillage and maintains adequate records management.

USAID prefers that employees and contractors utilize the soft token solution due to cost, security, and green initiatives. USAID employees, Personal Service Contractors (PSCs) and institutional contractors are limited to soft tokens unless they are unable to utilize a soft token due to security constraints. Hard tokens may be issued when required by security constraints.

Please see the M/CIO IT Services site for guidance on support provided by the M/CIO Service Desk in regards to remote access.

Please note: M/CIO is not responsible for technical support of personal devices. Therefore, M/CIO will not be able to:

- Troubleshoot any issues not related to the remote access with your personal device;
- Install any application or remove any applications on personal devices not related to remote access; and
- M/CIO also is not responsible for software incompatibilities caused by the installation and usage of the remote access applications software on your personal device.

Contact the M/CIO Service Desk at (**cio-helpdesk@usaid.gov**) to be issued a token. Tokens must be used at least once every 30 days to avoid having the account disabled.

For additional information on the acceptable use of hard or soft tokens please see **ADS 547, Property Management of Information Technology (IT)** and **ADS 545mbd, Rules of Behavior for Users**.

549.3.5.2 Electronic Messaging
Effective Date: 03/09/2016

The Federal Records Act Amendments of 2014 (**44 U.S.C 2911**) defines electronic messages as electronic mail and other electronic messaging systems that are used for purposes of communicating between individuals. Official Agency electronic messaging allows users to read, compose, send, and store messages over a network to USAID internal and external individuals, groups, or organizations. As defined in NARA Bulletin 2015-02, electronic messaging (EM) includes all forms of email (electronic mail), texts, instant messages/chats, social media messaging systems, and voice message platforms. USAID further defines electronic messaging systems as tools, platforms, applications, or other systems used to conduct official business. See **ADS 545** and **ADS 545mam, Acceptable Use Policy for Information Technology Resources** regarding USAID's policies and procedures on the use of USAID email. See **ADS 502.3.4.6 (Electronic Messaging)** for guidance on electronic messaging requirements.

549.3.5.3 Acceptable Use of the Internet
Effective Date: 12/15/2015

The following policies and essential procedures cover the use of the Internet through connections or GFE that are provided or owned by USAID. **ADS 545** and **ADS 545mar, Internet Acceptable Usage Policy** applies to all USAID users who access the Internet through USAID's computing or networking resources. The Agency's Internet users are expected to be familiar with, and to comply with this policy.

M/CIO may allow or deny access to external Internet sites/services as business needs change or conditions warrant. All services not expressly authorized by M/CIO will be considered unauthorized access to/from the Internet and will not be allowed.

1) USAID staff are authorized to use the USAID Internet if they have been issued a USAID PIV or PIV-A card, network account and USAID provided computer. People without a USAID network account or utilizing a non-USAID computer may access the Internet via the USAID Guest Network, where available. Access to the USAID Guest Network must be facilitated through their sponsor or the B/IO AMS Officer or Mission EXO.

2) The Internet must be used for unclassified purposes only. Classified, national security information is not permitted on the Internet.

3) Use of the Internet for destruction of United States Government (USG) property, harassment or criminal acts is prohibited and will be punishable by applicable U.S. and host- country laws.

4) Use of the Internet must be consistent with the Agency's policy on computer network access, use, and security restrictions (see **ADS 545**). This includes abiding by the Agency's computer security policies and essential procedures.

5) Freeware/shareware downloading from the Internet is not permitted under current USAID policy (see **ADS 545**).

USAID employees and contractors must all follow the **Rules of Behavior for Users** for Internet and intranet usage (see **ADS 545** for additional guidance on Acceptable Use of the USAID Internet, use of social media and social networking, file sharing and Voice over Internet Protocol (VoIP)).

549.3.5.4 Freedom of Information Act (FOIA)/Privacy Act

Effective Date: 12/15/2015

All printed or electronic materials (*e.g.,* email messages, g-chats, texts on Agency mobile phones, etc.), whether they pertain to official government business or are personal in nature, are subject to requirements of FOIA and the Privacy Act of 1974. Users of the USAID systems have no reasonable expectation of privacy for any communications or data transiting or stored on this information system. At any time, the government may for any lawful government purpose monitor, intercept, search, and seize any communication or data transiting or stored on this information system. See **ADS 508, Privacy Program** and **ADS 541, Information Management** for additional guidance. Printed or stored email or text messages, which are the subject of a FOIA request, must be reviewed in exactly the same way as any other record (see **ADS 507, Freedom of Information Act** and **ADS 502, The USAID Records Management Program** for further guidance).

549.3.5.5 Specialized Telecommunications Services

Effective Date: 12/15/2015

M/CIO must evaluate requests for value-added telecommunications services (*i.e.,* services for which the Agency must acquire specialized services such as IT services for USAID conferences or video sign language interpreter, and/or incur additional costs for access) and determine if any additional hardware, software, or telecommunications bandwidth are required. B/IOs and Missions may request these services by contacting the M/CIO Service Desk (**cio-helpdesk@usaid.gov**). The requesting B/IO or Mission may incur additional costs.

M/CIO provides Video Teleconferencing (VTC) services to USAID/W, B/IOs, and Missions. VTC devices are installed in USAID/W and Missions allowing USAID staff to connect with the Department of State sites, other federal agencies, NGOs, private organizations, and universities. B/IOs must submit an M/CIO Service Desk ticket (**cio-helpdesk@usaid.gov**) to schedule a VTC teleconference 10 business days in advance of the meeting. This is necessary to ensure adequate telecommunications facilities are available.

549.3.5.6 USAID Intranet

Effective Date: 12/15/2015

The USAID intranet provides access to internal USAID applications, document management systems, social media platforms and knowledge management systems. The use of these systems operates under the direction and guidance of **ADS 545** and **ADS 508**.

Usage of the intranet is subject to the Agency's monitoring; and unauthorized or improper user of the intranet may result in disciplinary action. While some of the intranet elements may resemble social media platforms that are utilized external to the Agency, the intranet is a USAID program that may be used only for official Agency purposes. Thus, engagement must be limited solely to activity that advances the Agency's development mission. Users must understand that all information posted to or generated by the intranet is subject to public review through a FOIA request or other demand. SBU and Personally Identifiable Information (PII) should be handled according to **ADS 508** and the **Privacy Act of 1974**.

549.3.5.7 Data Wiring

Effective Date: 12/15/2015

All Agency wiring must be carried out per Federal Information Processing (FIP) standards, state and county regulations, and in compliance with equipment manufacturer specifications.

All requests for domestic data wiring or cabling must be submitted in writing to M/CIO Client Services at **clientservices@usaid.gov**. M/CIO will make arrangements for installation and testing.

Individuals are prohibited from disconnecting or connecting any telecommunications equipment in USAID/W without explicit authorization from M/CIO. In USAID/W, only authorized M/CIO employees and contractors are permitted to install, connect, or disconnect any telecommunications or data communications equipment including end user computing devices (*e.g.,* computers, printers, telephones, etc.), or physically reconfigure the network.

Only System Managers overseas will be permitted to manage the equipment currently connected to the network (which might require disconnecting/connecting equipment for repairs, reconfiguration, etc.). See **ADS 547, Property Management of Information Technology (IT)**, **ADS 527maa, Guidance on How to Open a USAID Mission** and **ADS 527mab, Administrative Guidance on How to Close a USAID Operating Unit – Checklists** for additional information on data wiring and cabling at Missions.

549.3.5.8 USAID Network (AIDNET) Management

Effective Date: 12/15/2015

M/CIO will manage the Agency's Telecommunications Network (AIDNET) consistent with **ADS 552, Cyber Security for National Security Information (NSI) Systems** and **ADS 545**.

Individuals at overseas locations who are authorized to access AIDNET must adhere to the regulations outlined in **ADS Chapter 565, Domestic Security Programs** and local Mission policies and regulations.

Overseas Missions connected to AIDNET must be delegated responsibility for managing local network resources and coordinating AIDNET services with the central AIDNET Network Operations and Management Group within M/CIO. The Mission systems manager is expected to perform local network functions and duties. For purposes of emergency diagnostics of network problems, M/CIO must be provided credentials necessary to access each server connected to the AIDNET.

M/CIO must be the coordinator for registration of all federal and international telecommunication address assignments for the Agency.

M/CIO must provide the tools for Mission IT Specialists to perform basic utilization reporting for their platforms and conduct periodic reviews on disk utilization, line activity, concentrator workload, server performance, and evaluate new maintenance releases for the operating system software. Corrective actions must be taken by either the IT Specialist or M/CIO when problems are encountered. M/CIO must disconnect individual servers if problems are encountered that have the potential of affecting the overall performance of AIDNET.

International access to the Agency's telecommunications network (AIDNET) must depend on a variety of conditions and options that will be addressed on a case-by-case basis. M/CIO must, in coordination with the Mission and other M/CIO divisions, assist in determining the requirements and the best method to support the Agency's telecommunications requirements.

The requirements taken into consideration to determine connectivity needs are the size of the Mission, quality of local telecommunications services, proximity to the local Embassy, anticipated volume of data traffic, and amount of email exchanged with the AIDNET community outside the Mission. For locations where there is no Agency Mission, but Agency representation, connectivity requirements to AIDNET must be handled on a case-by-case basis.

549.3.5.9 Internet Protocol Version 6 (IPv6) Compliance

Effective Date: 04/12/2021

Internet Protocol version 6 (IPv6) is the most recent version of Internet Protocol (IP). IPv6 is the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.

Effective no later than Fiscal Year (FY) 2023, all new networked Federal information systems must be IPv6-enabled at the time of deployment. The use of IPv4 will be phased out across Agency Federal Information Systems. System Owners must work with B/IO/M leadership to allocate adequate funding to support the refresh, as

necessary, of the IP-enabled assets associated with their systems to fully enable native IPv6 operation by the end of FY25 (see **OMB M-21-07**).

This policy applies to all current USAID systems and new USAID acquisitions of IT products or services using Internet Protocol (IP). B/IO/Ms planning to procure an IT product or service using IP must include the appropriate IPv6 requirements language in the procurement request. B/IO/Ms must notify the Contracting Officer (CO) of these IP requirements. The CO must then include the appropriate special contract requirement in the solicitation and resulting contract (for current language see **AAPD 16-02 Revision 2**).

For additional guidance, please contact M/CIO Client Services Intake at **https://usaiditsm.servicenowservices.com/sphome?id=sc_cat_item&sys_id=bfd3b3b2db30df40e2c0fd0e0f96190f**.

549.3.5.10 Access Methods

Effective Date: 12/15/2015

The access methods described in the following essential procedure offer the capability to meet current requirements of unclassified telecommunications security.

DOS DTS-PO Provided Connectivity: To implement DOS/Diplomatic Telecommunications Service Program Office (DTS-PO) communications service, M/CIO must officially request Agency connectivity on behalf of the Mission. Determination and authorization to implement DOS/DTS-PO service at a given Agency location lies solely with the DOS/DTS-PO and depends on bandwidth availability. Missions must not request service directly from the local Embassy Information Process Office (IPO).

DOS/DTS-PO provided connectivity is a secondary or backup communication path at Missions, with the primary method being a local Internet Service Provider (ISP) Internet connection. The DTS-PO communication path is also used by USAID to transport Voice Over Internet Protocol (VOIP) traffic.

549.3.5.11 Satellite Communications Connectivity

Effective Date: 12/15/2015

Satellite services provide reliable communications for posts that have no other alternative. Satellite services are funded, procured, and deployed to a given overseas Mission by M/CIO in conjunction with the Mission.

Satellite connectivity must support data, voice (including facsimile), and video network traffic. To implement satellite communications capabilities, the satellite service provider will:

- Ensure the functionality of the USAID Mission satellite dish;
- Supply and maintain the satellite modem located at the Mission;

- Ensure adequate bandwidth is reserved and operated on each satellite to support Mission connectivity;

- Monitor and maintain the operations of the network link from each demarcation point (Mission: Satellite Modem; CONUS: AIDNET hand-off at provider location);

- Support Mission relocations and new implementations; and

- Deploy technicians to repair inoperable equipment and links.

To implement satellite communications capabilities:

- USAID Missions must obtain clearance from the Regional Security Officer (RSO) and in-country clearance (if required by the RSO) from the appropriate ministry for telecommunications services; and

- The primary satellite communications system managed by M/CIO for AIDNET is primarily funded by USAID/W. However, if a USAID Mission requires additional or dedicated satellite communications connectivity, they must contact the M/CIO Service Desk. USAID Missions must fund all costs for hardware, software, start-up temporary duty (TDY) support, and connect-time commercial carrier charges for any additional or dedicated systems, which will be billed on a usage basis.

549.4 MANDATORY REFERENCES

549.4.1 External Mandatory References

Effective Date: 12/15/2015

a. **5 FAH-2 H-212, What Subject Matter Can Go In A Telegram?**

b. **12 FAM 540**

c. **31 U.S.C Sec. 1348, Telephone Installation and Charges**

d. **Federal Property Management Regulation (FPMR), Subpart 101-35.1, Section 101-35.202**

e. **Foreign Affairs Manual (FAM) 500, 540, 665, 1200**

f. **Privacy Act of 1974**

g. **The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C Sec. 1801 et seq.)**

h. The Omnibus Crime Control and Safe Streets Act of 1968, as amended (18 U.S.C Sec. 2519 et seq.)

i. United States Intelligence Activities, E.O. 12333, or any successor order

549.4.2 Internal Mandatory References
Effective Date: 05/18/2017

a. ADS 501, The Automated Directives System (ADS)

b. ADS 502, The USAID Records Management Program

c. ADS 507, Freedom of Information Act

d. ADS 508, Privacy Program

e. ADS 527, Functions of the Mission Executive Officer

f. ADS 527maa, Guidance on How to Open a USAID Mission

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

h. ADS 545, Information Systems Security

i. ADS 545mam, Acceptable Use Policy for IT Resources

j. ADS 547, Property Management of Information Technology (IT) Resources

k. ADS 552, Cyber Security for National Security Information (NSI) Systems

l. ADS 565, Domestic Security Programs

m. USAID Agency Notice 03198: Information Technology Asset Management - Employee Separation and Transfer Procedures Agency Notice

549.5 ADDITIONAL HELP
Effective Date: 12/15/2015

There are no Additional Help documents for this chapter.

549.6 DEFINITIONS
Effective Date: 04/12/2021

See the ADS Glossary for all ADS terms and definitions.

agency profiles

A list of key subject-matter words that are of interest to organizations. (**Chapter 549**)

channel captions
Restrict action telegrams to designated offices or individuals in USAID/Washington (USAID/W) or USAID Missions. (**Chapter 549**)

commercial telegrams
Telegrams that are sometimes sent to international or domestic addresses that do not have access to governmental telegraphic facilities. In such cases, delivery is by commercial telegraphic systems. The Department of State (DOS) uses commercial telegram systems only for domestic locations. (**Chapter 549**)

data telecommunication
This includes local area networks (LANs), wide area networks (WAN), mainframe, mini and gateway microcomputers, electronic bulletin boards, electronic mail (email), X.400, Internet, and other network-enabled applications provided through the USAID Network (AIDNET) (*e.g.,* sending faxes through email, asynch dial-out/dial-in, File Transfer Protocol (FTP), telecommunication network, etc.) for both USAID/W and overseas locations. (**Chapter 549**)

domestic voice telecommunications
Voice telecommunications originating and ending within the United States. (**Chapter 549**)

flash
Outgoing telegrams that are to be delivered instantly (state of emergency) any day or night. (**Chapter 549**)

immediate
Outgoing telegram label assigned to important policy or end of life matters. (**Chapter 549**)

interested party messages
A method of transmitting telegrams when the Agency has indirect interest in the subject matter. This method is most commonly used to provide assistance to private individuals or companies overseas. In most cases, the Agency rarely initiates this type of telegram. (**Chapter 549**)

International Voice Gateway (IVG)
The Department of State's (DOS) private network for telephone calls that links U.S. Embassies (and the U.S. Missions that get their phone service from the Embassy) with USAID/W and DOS. (**Chapter 549**)

Internet
The collection of interconnected networks that connect computers around the world. (**Chapter 545** and **549**)

Internet Protocol Version 6 (IPV6) IPv6
A set of specifications from the Internet Engineering Task Force (IETF) that is an upgrade and a replacement for IP version 4 (IPv4). Both refer to the standard used in addressing information systems, computers and other similar devices to facilitate the transmission and reception of information. (**Chapter 545**, **509**, and **549**)

Message Reference Number (MRN)
The official reference number assigned by the Communications Center to telegrams. It appears following the classification beneath the last addressee and consists of the originator's name and organization (not abbreviated), followed by a multi-digit number (*i.e.,* STATE 123456; BONN 3597). (**Chapter 549**)

minimize
A telegram control procedure imposed during emergency conditions (*i.e.,* local civil disorders; communications circuit failures; natural disasters) to reduce the volume of traffic not related to the emergency and to avoid overloading the communications facilities and personnel capabilities of the department and the affected post(s). A current list of posts that are on "MINIMIZE" is maintained at the Communications Center. To find out what is on "MINIMIZE", call (202) 712-5981. (**Chapter 549**)

NIACT/immediate
The marking for outgoing telegrams that are to be delivered immediately - any day or night. (**Chapter 549**)

priority
Outgoing telegrams that contain essential information for operations and actions in progress. (**Chapter 549**)

reference line
Use a reference line to refer to a previous telegram or line related communication. Although there is no limit to the number of references or lines, the Department's automatic retrieval system recognizes telegram references on only one line. References placed on succeeding lines will remain part of the telegram but cannot be used in automatic retrieval. (**Chapter 549**)

routine
Outgoing telegrams with the lowest order of precedence assigned to communications which justify DOS transmission but are of insufficient urgency to require a higher precedence. (**Chapter 549**)

software (soft) token
A two-factor authentication security device that may be used to authorize the use of computer services. Software tokens are stored on a general-purpose electronic device such as a desktop computer or mobile computing device. (**Chapter 549**)

subject line
The subject line, assigned by the originator, highlights message content; identifies reader interest; and helps to automatically retrieve the telegram. Assign a subject that is concise but gives clear clues. (**Chapter 549**)

telecommunications equipment
This includes telephones, mobile phones, facsimile machines, and computer equipment attached to the network. (**Chapter 549**)

telecommunications network
This includes email, development and dissemination of directory management procedures, network design and features, coordination of installation of local area networks (LANs), and utilization monitoring and performance management. (**Chapter 549**)

telegram captions and attention indicators
A four-letter computer address assigned by the Communications Center to an Agency office which designates the action office. (**Chapter 549**)

telegram communication
(Commonly known as the Cable System) includes all activities involving the coordination of telegram regulations with other government agencies, preparation and distribution of all Agency telegrams, and maintaining hardware and software to support the operation of the telegram system. (**Chapter 549**)

telegram precedence indicators
Prescribe the relative urgency for handling and transmitting telegrams. (**Chapter 549**)

USAIDAC
This term is used when the subject of the outgoing telegram has to do with USAID programs or projects, or other substantive matters that are of interest to other U.S. Government agencies. (**Chapter 549**)

USAID Network (AIDNET)
This includes: a) electronic mail (email), the development and dissemination of directory management procedures; b) network design and features; c) coordination of installation of local area networks (LANs); and d) utilization monitoring and performance management. (**Chapter 549** and **550**)

value-added telecommunication services
This includes activities such as IT support at USAID conferences, video conferencing, direct connections to other U.S. Federal or State Government entities, NGOs, or commercial companies. (**Chapter 549**)

voice communication

This includes telephones, pagers, long-distance calling, facsimile machines, and voice mail for USAID/W sites. (**Chapter 549**)

Voice over Internet Protocol (VoIP)
USAID's private phone network that enables calls between USAID/W and the Missions. VoIP is usually available at posts where IVG is not available. Missions may also use it to call anywhere in the U.S. for free. (**Chapter 549**)

549_041221