ADS Chapter 552

Cyber Security for National Security Information (NSI) Systems

Full Revision Date: 09/26/2017
Responsible Office: M/CIO/IA
File Name: 552_092617

Functional Series 500 – Management Services
ADS 552 – CyberSecurity for National Security Information Systems
POC for ADS 552: Angel Cruz, ancruz@usaid.gov, (202) 712-5989 or Bruce Wierzechowski Sr., bwierzechowski@usaid.gov, (202) 657-1878

This chapter has been revised in its entirety.

Table of Contents

ADS 552 – National Security Information Systems Information Security Programs

552.1 OVERVIEW

Effective Date: 09/26/2017

This ADS chapter applies to the USAID workforce, regardless of employment category or access capacity, who are granted access to classified information-technology (IT) media, systems, and/or resources under the control of, or in use at, USAID Washington (USAID/W). All classified IT activities, regardless of classification level, are under the purview of this ADS chapter. Throughout this chapter, the term "workforce" 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 Direct-Hire employees, Personal Services Contractors, Fellows, Participating Agency Service Agreements (PASAs), and contractor personnel. Contractors are not normally subject to Agency policy and procedures as discussed in **ADS Chapter 501**. However, contractor personnel are included here by virtue of the applicable clauses in the contract related to Homeland Security Presidential Directive (HSPD)-12 and Information Security requirements.

For purposes of this document, Information Systems Security (ISS) has the following meaning: the protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information systems security is comprised of computer security and communications security.

This chapter implements comprehensive local policies and standards to adequately safeguard and protect USAID classified data, national security information (NSI) systems, and operational environments. This ADS chapter governs all:

- Classified data sharing and processing;
- Onsite or telephonic classified discussions, conversations, and meetings;
- Classified secure video-teleconferences; and
- Classified electronic transmissions.

This policy levies minimum federal regulatory mandates as well as Agency- and service-provider baseline security requirements.

At a minimum, members of the workforce who are granted access to classified national security information, systems, resources, facilities, media conferences and/or conversations must hold a current and valid clearance that is equivalent or higher than that of the information or resources that will be accessed.

552.2 PRIMARY RESPONSIBILITIES

Effective Date: 09/26/2017

a. The **Administrator** has delegated the information systems security (ISS) program compliance responsibility, role, and related activities to the Bureau for Management, Office of Chief Information Officer (M/CIO) (see **ADS 103, Delegations of Authority**).

b. The **Chief Information Officer (CIO)**:

(1) Has signatory "Authority to Operate" (ATO) approval for all Agency information systems;

(2) Acts as the USAID classified computer systems operations Approving Official (AO);

(3) Ensures uninterrupted secure telecommunications;

(4) Appoints a primary and an alternate Information Systems Security Officer (ISSO), who ensures comprehensive information assurance (IA) and ISS governance;

(5) Maintains ongoing visibility and awareness of Agency secure communications, security posture, and vulnerability management; and

(6) Maintains current and future Agency telecommunications policies and procedures ensuring alignment with the Agency IT strategic direction.

b. **Assistant Administrators (AAs) and Office Directors** must formally, in writing, provide M/CIO with an appointee that will act as the B/IO ISSO and have these following responsibilities:

(1) Promulgate, ensure, and enforce adequate protection of national security data, information, information systems, resources, and media (regardless of creation, storage, transmission, dissemination, and platform);

(2) Report ISS infractions to the M/CIO ISSO; and

(3) Ensure access to classified telecommunications systems is in alignment with **Executive Order (EO) 13526** Section 4.1.requirements.

c. The **Chief Information Security Officer (CISO)**:

(1) Has oversight over all B/IO ISSOs; and

(2) Is responsible for ensuring the logical and technical security posture and

compliance of the classified network and operations (see **ADS 545, Information Systems Security**, and **ADS 561, Security Responsibilities**).

d. An **Information System Security Officer (ISSO)** is an M/CIO designated individual responsible for ensuring that the appropriate operational security posture is maintained for an information system and as such, works in close collaboration with the information system owner. The ISSO also serves as a principal advisor on all matters, technical and otherwise, involving the security of an information system. The ISSO has the detailed knowledge and expertise required to manage the security aspects of an information system and, in many organizations, is assigned responsibility for the day-to-day security operations of a system.

e. The **Office of Security (SEC)** is responsible for conducting and confirming the preliminary inquiry into an IT security incident in coordination with M/CIO when Data Spillage or Spillage occurs on ClassNet, JWICS, or unclassified systems.

f. **USAID workforce** who are granted classified telecommunications access must:

(1) Meet access requirements as outlined in **EO 13526** and **12 FAM 600**, **12 FAM 610**, **12 FAM 630** for classified providers network; and

(2) Report known, suspected, or perceived problems or incidents that could impact the confidentiality, availability, or integrity of the classified systems and data.

g. **Contractor Officer's Representatives (CORs)** have a key role in ensuring that cost-effective information system security (ISS) processes and features are incorporated into IS products and services. CORs represent the product or service requestor in the acquisition process. CORs also lead the development of sensitivity assessments for the systems and data associated with the contract and work with the designated ISSO to ensure that the appropriate levels of protection are applied to the contract.

h. **Administrative Management Staff/ Executive Management Team (AMS/EMT) Officers** are responsible for initiating all B/IO ClassNet account access and classified phone requests. B/IO AMS/EMT Officers must work with the ClassNet Team to ensure that Public Key Infrastructure (PKI) tokens, secure phone and crypto cards are returned to the Classified Support Team when any member of the USAID workforce no longer has a valid need to have access to ClassNet or upon separation from the Agency.

552.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

552.3.1 Information Systems Security Program Authority

Effective Date: 09/26/2017

Federal departments and agencies must develop and implement a comprehensive, Agency-wide Information Systems Security (ISS) program that is technically current, cost effective, and in full compliance with applicable, currently published statutes, federal laws, National Security Directives (NSDs), and **Executive Order 13587** (see **552.4**).

552.3.2 Information Systems Security Program Accountability
Effective Date: 09/26/2017

Heads of federal agencies may delegate activities and roles but must not transfer their responsibilities for confidentiality, integrity, availability, safeguard, and protection of National Security Information (NSI) resources and information sharing.

552.3.3 Information Systems Security Program Responsibility
Effective Date: 09/26/2017

The Administrator has delegated the ISS program compliance responsibility, role, and related activities to the Bureau for Management, Office of Chief Information Officer (M/CIO). This delegation of authority includes, but is not limited to IT assets funded by USAID, even if provided or managed by another agency, contractor, or other source. The Chief Information Officer (CIO) has delegated responsibility to the USAID Chief Information Security Officer (CISO) to execute the ISS program (see **OMB 11-29, Chief Information Officer Authorities, 8/8/2011**, **44 USC 3506, 01/03/2012**). The CISO is required to conduct, document, and report the Agency-wide compliance of all IT systems (unclassified and classified) per the **Federal Information Security Management Act of 2002** and the **Federal Information Security Modernization Act of 2014**.

This compliance is achieved by meeting the minimum security requirements of all applicable governance and Information Assurance (IA) security controls that govern people, processes, technologies, and facilities that house U.S. Government IT systems per **NIST 800-53**, **CNSS**, **12 FAM 600**, **12 FAM 610**, **12 FAM 630**, and Defense Intelligence Agency (DIA) (please contact **classnetrequests@usaid.gov** for further information on DIA controls).

552.3.4 Classified Networking Environment
Effective Date: 09/26/2017

The Classified Network (ClassNet) is a Department of State (DoS) owned system that extends its service into USAID/Washington (USAID/W). The ClassNet system is sponsored by M/CIO and managed by the M/CIO/CISO/IA/SO, Classified Enclave Information System Security Officer (ISSO). It is a collection of local workstations networked together and connected to remote classified servers maintained at the DoS via encrypted circuits that process information up to the Secret level. ClassNet is independent of all USAID unclassified networks (computing systems, printers, scanners, and telephones).

Please review the **Classified Support Site** as well as **552.3.8** for additional guidance.

552.3.5 Procurement of IT Hardware and Software

Effective Date: 09/26/2017

The following is the policy for USAID's acquisition of computer hardware, software, and peripherals for processing national security information (NSI):

- B/IOs must adhere to the Department of State Classified System Owners IT Configuration Control Board (ITCCB) (for additional information please contact the Department of State's IT Help Center at 202-647-2000);

- All Agency personnel acquiring classified equipment must obtain B/IO leadership approval and submit IT acquisition approval requests to **classnetrequest@usaid.gov**;

- The Classified Support Team and AMS Officers must issue and obtain signed hand receipts for all issued classified IT equipment issued to users to ensure that equipment is accounted for and tracked in the IT inventory;

- AMS Officers must assist the Classified Support Team in conducting monthly inventories of classified IT equipment; and

- Only M/CIO is authorized to procure computer hardware, software, and peripherals for processing national security information (NSI).

Procurement of IT equipment that is intended to process NSI is strictly prohibited. Any IT assets procured without following this ADS chapter violates IT security and will result in actions such as auditing or loss of access to the IT system. M/CIO may mandate that the B/IO procure a replacement M/CIO-authorized system at their expense.

552.3.6 IT Security Incidents (IT Incident Response)

552.3.6.1 Prohibited Procedures for Handling Classified National Security Information on Information Technology Systems

Effective Date: 09/26/2017

Individuals must not process, download, or transfer classified data (Confidential (C), Secret (S) or Top Secret (TS)) to unclassified systems or their personal devices (see **18 USC 1924, Unauthorized Removal and Retention of Classified Documents or Material**; **ADS 405, Telework**; **ADS 568**; **ADS 566, Personnel Security Investigations and Clearances**; and **12 FAM 533, Removing Classified Material from Official Premises** for additional guidance).

If an individual processes or creates a classified document at their alternative worksite,

spillage has occurred. Data Spillage or Spillage is the transfer of classified information to unaccredited or unauthorized systems, individuals, applications, or media. The data itself may be residual (hidden) data or metadata. In the event of a spillage incident, the Office of Security (SEC) must conduct the preliminary inquiry and coordinate with M/CIO. M/CIO must conduct a forensic review of the individual's personal electronic device, which may result in wiping all data and software stored on personal electronic devices up to and including completely wiping or physical destruction of the personal device in cases of classified spillage (see **NIST SP 800-88, Guidelines for Media Sanitization**).

552.3.6.2 IT Financial Management and Spillage Cost Recovery

Effective Date: 09/26/2017

The purpose of the USAID IT security incident program is to enhance the protection of classified information by identifying, evaluating, and reporting breaches of IT security (see **ADS 568** to review disciplinary actions related to security infraction and **ADS Chapter 569, Counterintelligence Program** for guidance on incident response activities).

B/IOs responsible for classified spillage must provide cost recovery to M/CIO for each incident. Recovery costs must comprehensively reimburse M/CIO for all levels of effort to respond to, and recover from, each incident; including personnel, budget, hours, hardware/software cleanup/recovery/replacement, etc. M/CIO must document all incident response activities, levels of effort (LOE), and costs. M/CIO will maintain LOE and costs as evidence associated with each incident when requested. LOE reimbursement costs must be billed to the responsible B/IO, and, where applicable, the responsible individual. AAs and Office Directors accountable for cost recovery must ensure timely cost reimbursement to M/CIO, normally within 30 business days of awareness/receipt of recovery costs.

Incidents must be submitted by emailing (a) **classnetrequests@usaid.gov**, (b) **CIO ISSO@usaid.gov**, (c) **csirt@usaid.gov**, (d) **SECInformationSecurity@usaid.gov**, (e) **SECDomestic@usaid.gov**.

552.3.7 IT Security Inspections and Assessments (Audit and Accountability)

Effective Date: 09/26/2017

Per the Committee on National Security Systems (CNSS) or provider policy, M/CIO is responsible for conducting periodic assessments that document, report, and track compliance of applicable information assurance security controls across the Agency.

Inspections must include, but are not limited to the overall Agency operational security posture, and includes logical, physical, technical, administrative and operational security devices, controls, configurations, baselines, policies, standards, and processes and procedures against current regulatory standards and industry best practices.

Any security deficits discovered must be documented, reported, mitigated to the lowest possible or acceptable level in a timely manner, tracked, and closed, where feasibly possible. Security inspection checklists and audit tools can derive from local or external resources, but, at minimum, they must comply with current versions of regulatory mandates. B/IOs must report security deficits to their AA or Office Director of non-compliant B/IO(s). The AA or Office Director must first acknowledge receipt and then must implement, track, and report progress of corrective action(s) through closure to the CIO ISSO, and to service provider(s), where applicable, quarterly. Failure to do so could result in interrupted classified communications to the B/IO and/or the Agency.

Cleared, U.S. citizen IT security representatives designated by M/CIO are responsible for conducting and documenting joint, announced and unannounced, periodic IT security system inspections. The purpose is to ensure B/IOs:

- Adequately and properly safeguard and protect NSI; and

- Conduct such security inspections for all offices, buildings, or other facilities under USAID CONUS (Continental United States) jurisdiction.

M/CIO ISSOs must randomly review selected storage media and system hardware associated with information systems under their purview to ensure that users:

- Process information classified at the level authorized on the system;

- Process classified information only on authorized systems and equipment; and

- Use proper and visible labeling.

This section details random security inspection audits conducted by the M/CIO ISSO. B/IOs must document and retain evidence of random and annual security reviews. In addition, B/IOs must provide copies upon request to CIO ISSO, M/CIO, and/or service provider(s).

B/IOs and the M/CIO ISSO must adhere to the following:

- B/IOs must constantly observe the facility's condition via checklists and procedures provided by the M/CIO ISSO. The M/CIO ISSO must audit and enforce such activities. B/IOs that require the checklists and procedures must submit a request to **classnetrequest@usaid.gov**.

- Each B/IO must follow USAID and service provider procedures to report any maintenance, security, or safety concerns.

- Audits and/or assessments must address the Common Body of Knowledge (CBK) security domains and all applicable security controls mandated or required

by USAID and/or the service provider(s).

552.3.8 Disposition of Excess Equipment

Effective Date: 09/26/2017

All B/IOs and M/CIO ISSOs must adhere to M/CIO's requirements to establish and maintain accountability and management of tangible USAID and service-provider-owned equipment and other accountable property (see 12 FAH-6 for disposition requirements and processes).

552.3.9 File/Data Transfers (System and Communications Protection)

Effective Date: 09/26/2017

This section ensures adequate safeguard and protection during transmission or transfer of classified and unclassified information onto network systems operating at different classification levels through the use of electronic transmissions or copying data onto removable media.

Transferring data between different classification levels is termed as "a cross-domain data transfer." Specific processes and tools must be used to accomplish cross-domain data transfers. Please contact the M/CIO ISSO via email at: **classnetrequests@usaid.gov** or contact the M/CIO Service Desk for appropriate guidance at (202) 712-1234.

Cross-domain data transfers are unauthorized by any other Agency personnel, regardless of hire or support capacity (see **Moving document(s) from AidNet to ClassNet** for additional guidance).

M/CIO must ensure that trained representatives (e.g., trusted agents) are versed in and follow the classified system owner's policies, processes, and procedures for managing and supporting a given classified system for use within the Agency.

552.3.10 Requesting to a Classified IT System

Effective Date: 09/26/2017

Per **EO 13526 Section 4.1**, supervisors, prior to access, must validate and formally authorize initial system access requests on the currently approved and signed **System Authorization Access Request (SAAR)** and review user access annually. Note: the SF-312 (Non-Disclosure Agreement) does not serve as authorization to access classified national security information.

B/IO supervisors or Contracting Officer's Representatives (CORs) must include language on the post-checkout list, or out-processing documentation (**AID Form 451-1** for Direct Hires, PASA/RASAs, PSCs, Interns or Fellows) to ensure timely M/CIO ISSO notification of all transferred or terminated members of the Agency workforce. The CIO ISSO and SEC must ensure classified telecommunications access to ClassNet, Joint

Worldwide Information Communications Systems (JWICS), or other classified systems is terminated upon notification of transfer or termination.

Supervisors or CORs must:

- Validate annually that each user, who has NSI access, still requires access to NSI for official Agency duties;
- Ensure that contractor access does not exceed the contract period of performance;
- Identify, document, and report access modifications to ClassNet accounts to the M/CIO ISSO (via the currently approved SAAR) within 24 business hours of awareness; and
- Renew access requests for authorized users every three years from the original approved SAAR authorization date for all users, and/or at contract extension or renewal periods (whichever occurs first) for ClassNet. They must also contact SEC at secinformationsecurity@usaid.gov for JWICS.

The M/CIO ISSO must ensure that:

- Authorized users have access to individual user identifications (IDs) and passwords;
- Password complexity conforms to the service provider's policy; and
- Where feasible and available, Public Key Infrastructure (PKI) and Personal Identity Verification (PIV) technology must be implemented and mandatory.

552.3.10.1 Requesting Access to Classified Telephones

Effective Date: 09/26/2017

Users requiring assignment of classified telephones in restricted space must submit justification to the AMS Officer on why they require assignment of a permanent classified telephone. AMS Officers must review and validate the need and submit a service ticket to the Classified Support Team through the M/CIO Service Desk requesting that a classified telephone be assigned to a specific user. The Classified Support Team will contact the requesting AMS Officer for next steps.

552.3.11 Unacceptable Use

Effective Date: 09/26/2017

This section describes unacceptable use, in terms of planning, of NSI and systems.

The Agency workforce must not participate in unacceptable use of classified information

systems as referenced in **12 FAM 600**, **12 FAM 610**, and **12 FAM 630**.

552.3.12 Account Management (Access Control)

Effective Date: 09/26/2017

M/CIO manages the classified PKI program, manages classified access request forms, and forwards approved classified access request forms to the appropriate service provider for account creation and management. For guidance, please visit our **Classified Support Site**.

552.3.12.1 ClassNet Account Management (Requesting Access to NSI)

Effective Date: 09/26/2017

All System Access and Authorization Requests (SAARs) must be U.S. Government supervisor-approved, formally signed (where possible digital or PKI), and returned electronically to **classnetrequests@usaid.gov**.

SAARs must be processed by satisfying all mandatory access prerequisites via the **Classified Support Site**. If forms are not completed correctly, your request will be rejected and must be corrected and resubmitted for review and approval.

For each configured user, the M/CIO ClassNet ISSO must revoke and remove access when access is no longer authorized or required.

Accounts and access for classified IT elements (e.g., Network systems, data, and/or information resources) must be granted only to authorized persons with an approved security clearance determination (adjudication status) of FINAL and FAVORABLE, except where the USAID Administrator (A/AID) deems and formally justifies "exceptional need," in accordance with **EO 12968 Access to Classified Information**. Access requests for other-than-properly-cleared U.S. citizens must be authorized in accordance with **EO 12968** and communicated to and in coordination with M/CIO and SEC.

Compliance exceptions for users to access classified systems must be justified by a formal business case, allowable under federal statute or law, approved by the local Approving Official (AO), which is the Chief Information Officer (CIO), and by service provider(s)[1], and requires a formally documented, risk-based management decision.

For Classified National Security Information (CNSI) system, network, or resource users, the Office of Security must immediately notify the Office of Human Capital and Talent Management (HCTM) and M/CIO staff when a user's clearance has been temporarily or permanently revoked (see **ADS 566** for additional information).

U.S. Government supervisors and Contracting Officer Representatives (CORs) must notify the M/CIO ISSO within eight business hours of classified network user

[1] A Service Provider is an agency or entity that is providing a given classified service.

role/responsibility changes where it affects changes to access or access level(s).

AMS Officers must:

- Ensure U.S. Government supervisor approval and signature for all user access requests to classified resources, data, or information;
- Ensure that SAAR information is accurate and complete; and
- Coordinate, track, and submit all user access requests to **classnetrequests@usaid.gov**.

The M/CIO ISSO must receive, validate, and manage (beginning to end) authorization forms and validate that the forms are accurate and complete.

M/CIO must ensure classified service provider(s) adhere to formal Service Level Agreements (SLAs), Memorandums of Agreement (MOAs), and Memorandums of Understanding (MOUs).

552.3.12.2 Account Inactivity
Effective Date: 09/26/2017

Inactive accounts allow unauthorized entities time and opportunity to potentially gain access, alter, extract, manipulate, and potentially disclose NSI. M/CIO must ensure account access reviews are a part of their account management activities.

Note: To avoid having an account disabled, a user must, at a minimum, logon once every 30 days. USAID users must not circumvent USAID account management policy as outlined in **ADS 545, Information Systems Security** and **ADS 549, Telecommunications Management**. USAID users must contact **classnetrequests@usaid.gov** for assistance with disabled accounts.

- Accounts inactive for periods of 31 up to 90 days must be disabled. In order for an inactive account to be reactivated, the user's supervisor must submit a service ticket to the Classified Support Team through the M/CIO Help Desk requesting that the inactive account be reactivated.
- Accounts inactive beyond 90 days must be permanently disabled and users must reapply to reconstitute account access. There are no exceptions to this requirement.

552.3.12.3 Access Termination
Effective Date: 09/26/2017

Access termination is the formal process of terminating access when a user no longer requires access to classified IT resources. Please visit the **Classified Support Site** for

guidance on the deactivation process.

552.3.13 Inventory Management Program
Effective Date: 09/26/2017

The Chief Information Security Officer (CISO) must establish and maintain a sound inventory program that uniquely identifies NSI information technology assets.

B/IOs must:

- Support M/CIO in the annual IT asset inventory. Accountability practices include but are not limited to recording hardware serial numbers, software licenses, Agency barcodes, etc.;

- Submit a request to M/CIO for all classified IT equipment changes such as transfers, relocations, and disposals; and

- Immediately notify M/CIO ISSO, in the event of any loss or theft of IT assets.

552.3.13.1 Classified IT Asset Security Labels
Effective Date: 09/26/2017

The M/CIO ISSO must label all classified IT hardware prior to issuance. All classified IT equipment must be returned to the ClassNet ISSO when:

- No longer needed,

- Inoperative, and

- USAID no longer requires the connection.

M/CIO must record, coordinate, and ensure efforts to properly document, audit, and dispose of classified IT equipment through approved authorities and mechanisms (i.e., the National Security Agency (NSA), service provider, etc.).

552.3.14 Protective Distribution System (PDS)
Effective Date: 09/26/2017

Compliance with the guidance and standards for the design, installation, and maintenance of protected distribution systems contained in **NSTISSI No.7003, September 2015** (or its successor) is mandatory to protect all unencrypted national security information.

552.3.15 System Security and Maintenance
Effective Date: 09/26/2017

The M/CIO ISSO must ensure that required security patches and secure configuration baselines are accomplished in accordance with **FISMA**, **NIST SP 800-53 Rev. 4**, and Agency requirements. Members of the workforce must not modify any classified IT equipment without authorization from ClassNet ISSO.

B/IOs that maintain classified computers or printers with a removable hard drive must secure the hard drive outside of specific B/IO core hours in a GSA-approved container (safe) that is authorized to store information up to the classification level of the classified hard drive. If classified removable hard drives are found unsecured after B/IO core hours, the B/IO duty officer may be held responsible for improperly protecting classified information (see **ADS 568**). Unsecured hard drives found after hours must be reported to the Office of Security's Information and Industrial Security Branch at **secinformationsecurity@usaid.gov** or (202) 712-0990.

The M/CIO ISSO must maintain a log of all maintenance and service performed on NSI equipment. Electronic or hardcopy logs are acceptable and must be centrally maintained. For guidance on maintenance logs for classified NSI systems, please contact the M/CIO Service Desk.

M/CIO Classified Operations support staff must supervise vendor maintenance personnel, who must be U.S. citizens when they access NSI IT resources.

Citizens of specifically designated technical and/or human intelligence threat countries may not develop, modify, or perform maintenance on software used on government computer systems, unless there has been specific authorization from the service provider (see **12 FAM 633.1**).

Prior to disposition, transfer, or destruction, M/CIO must first wipe all IT to ensure there's no ghosting of metadata that could expose classified material (see **NIST SP 800-88, Guidelines for Media Sanitization**). The USAID Communications Security (COMSEC) Officer is the only official authorized to approve the release of the NSI IT equipment.

552.3.16 Classified IT Information Systems Security Briefing and Training

Effective Date: 09/26/2017

In accordance with **EO 13526** and current regulatory guidance (see **552.4**), agencies must adopt and implement security awareness, adequate safeguards, protection, and NSI-sharing programs to educate the Agency workforce concerning their duties and responsibilities. For guidance on how to apply for and to keep your classified account active, please visit the **Classified Support** Web site.

The M/CIO ISSO for USAID must provide, verify, and maintain all training required by regulatory governance, Agency, and service-provider policy. Upon request, the CIO ISSO for USAID must provide special training for other users who have security responsibilities for Agency classified systems.

552.3.17 Contingency Operations Planning (Contingency Planning)

Effective Date: 09/26/2017

M/CIO ISSOs must review, update (if necessary), and test all emergency action plans annually or when there are significant changes to system hardware, software, or personnel. Please see **ADS Chapter 531, Continuity of Operations Program** for guidance on the Agency's COOP Plan.

The M/CIO ISSO:

- Must retain copies of the most recent emergency action plans and contingency operation plans in the system's central file and at a designated backup site; and
- Must develop site-specific disaster recovery plans based on threat identification information, system resource accounting, and criticality assessment data.

552.3.18 Remote Access (Access Control)

Effective Date: 09/26/2017

Remote access to classified systems is prohibited - no exceptions.

552.3.19 IT Security Audits (Audits and Accountability)

Effective Date: 09/26/2017

M/CIO/IA Audit & Accountability Policy establishes a framework for conducting audit-related reviews of NSI resources, policies, procedures, process, and guidelines within USAID. B/IOs must adopt and adhere to M/CIO auditing standards for due care and due diligence.

B/IOs must conduct and adhere to monthly (as required), quarterly (as required), and required annual auditing of their respective classified processing facilities in accordance with M/CIO standards.

The M/CIO ISSO must ensure that, at minimum, the original information system (IS) security documents, logs, and records listed below are maintained, after processing, in a central file for each system authorized to process classified information:

- Classified Information System User Agreement (**AID Form 552-2**) and termination notices;
- Contingency operation, disaster recovery, and emergency action plans;
- Copies of waivers and/or exceptions;

- Security assessment and authorization (SA&A) documentation (as applicable);
- System maintenance logs;
- Documentation reviews for certification and accreditation;
- System authorization access requests and training records;
- M/CIO ISSO and alternate M/CIO ISSO appointment documentation;
- Annual classified processing compliance reviews (**AID Form 552-1**); and
- System inventories.

552.3.20 Communications Security (COMSEC)

Effective Date: 09/26/2017

COMSEC provides confidentiality, integrity, and availability to information in order to provide an uninterrupted secure communications capability.

The following policy statements apply to COMSEC.

USAID classified communications must be afforded maximum safeguards and protections both when in use and not in use. COMSEC staff must be certified in COMSEC operations, well trained in daily operations, and well versed in implementing effective, efficient communications security. Every effort must be made to ensure uninterrupted communications security. There must be timely, accurate inventory as well as key management and reporting. There must be informal and formal audits, coordinated as appropriate, and the CISO must formally report these audits to the proper Agency senior leaders and audit personnel.

Agency COMSEC custodians must provide over-the-counter (OTC) service to Agency B/IOs. This means that M/CIO COMSEC representatives must requisition, order, and deliver COMSEC equipment and key material OTC to properly trained, formally appointed B/IO COMSEC Responsible Officers (CROs). B/IOs that require COMSEC support must designate COMSEC support personnel from within their organization. B/IO leadership is responsible for ensuring that CROs receive both initial and event-driven training from M/CIO. Further, COMSEC designated support personnel must complete annual cybersecurity refresher training. B/IO designated CRO personnel must attend regularly scheduled CRO training. Noncompliance must result in COMSEC support suspension until training compliance is accomplished.

AAs and Office Directors must identify and verify training requirements as well as engage B/IO-appointed CROs to support B/IO COMSEC support requirements.

AAs and Office Directors must communicate COMSEC support requirements annually to COMSEC personnel and must formally appoint and maintain one primary and at least one alternate CRO at all times. Note: Two alternate CROs are strongly recommended.

AAs and Office Directors must ensure that CROs receive, remain available for, and maintain required CRO training, capability, and readiness.

AAs and Office Directors are directly responsible and accountable for ensuring COMSEC equipment and key material are adequately safeguarded, protected, and used in accordance with regulatory and service-provider governance. Further, the most senior B/IO leader is directly accountable for promptly reporting any instances of known, suspected, or anticipated COMSEC-related incidents, equipment, and/or key material compromise, loss, theft, or improper use. The most senior B/IO leader is responsible for managing and enforcing Agency COMSEC policy and for ensuring timely COMSEC communications and actionable CRO responses.

COMSEC users must realize and remain cognizant that COMSEC is a privilege extended to USAID and remains under strict accountability and control 24/7. Semi-annual (formal) and periodic (internal) inventory timelines must be met without exception. Not meeting reporting timelines places USAID in noncompliance with NSA-mandated reporting requirements and must not be tolerated. COMSEC personnel have full authority to inventory all COMSEC equipment and key material 24/7, with or without advanced notice. B/IOs must not impede any inventory efforts and must accommodate COMSEC representatives 24/7 or risk losing COMSEC support.

USAID is allowed a 10-day inventory issue and compliance report window without exception. Therefore, inventory extensions are not authorized and must be accomplished in the timelines provided.

COMSEC incidents must be reported directly, and only to COMSEC representatives as soon as any person is aware of any known, suspected, or potential incident of any category, scale, or scope. Where COMSEC personnel are known to be directly or indirectly involved with a COMSEC incident, the incident must be reported directly to any other Agency (not B/IO) COMSEC personnel or directly to the CISO. When COMSEC personnel or the CISO is available, COMSEC incidents must not be reported to any other personnel not directly involved in resolution, intervention, or without COMSEC need-to-know.

522.3.20.1 COMSEC Roles and Responsibilities

Effective Date: 09/26/2017

a. M/CIO must:

- Oversee implementation of this policy and ensure development of supplemental COMSEC policy as required; and

- Ensure that COMSEC activities:
    - Comply with applicable national policies and guidance;
    - Are compatible with planned and existing information systems;
    - Meet objectives for commonality, interoperability, compatibility, standardization, and survivability;
    - Review proposed COMSEC programs and the resource requirements as well as recommend resource allocations;
    - Plan, program, fund, implement, manage, and provide logistics support to the COMSEC requirements of B/IOs;
    - Establish and maintain a USAID-wide COMSEC assessment program to evaluate compliance with regulatory governance;
    - In the assessment, include management effectiveness of COMSEC incident reporting; and
    - Develop, maintain, and modify USAID policies, procedures, training programs, and software systems that ensure uniform application of the policies.

b. The COMSEC Office must:

- Oversee COMSEC cryptographic access, account management, processes, procedures, inventory, accountability, and activities;
- Review planned, existing, and emerging COMSEC technologies in relation to joint interoperability, plans, and objectives;
- Validate requirements for the COMSEC Utility Program (CUP) assets in accordance with service provider requirements;
- Direct Agency COMSEC practices;
- Oversee COMSEC operations, support, audits, reporting, and effectiveness; and
- Serve as the centralized COMSEC authority.

c. COMSEC custodians and alternates must:

- Review and validate all Agency COMSEC requirements and communicate and coordinate valid COMSEC requirements with the service provider;

- Coordinate and provide COMSEC support to the service provider for purchase/delivery/issuance and accountability of COMSEC material;

- Implement and manage all applicable COMSEC policies, directives, criteria, and standards;

- Serve as the service-provider COMSEC and cryptography focal point and manage the implementation of COMSEC policies and procedures throughout USAID CONUS facilities;

- In coordination with the service provider, implement established policies and develop plans, procedures, training, and mechanisms for all USAID COMSEC supporting personnel;

- Develop and implement methods, processes, procedures, and guidelines for training, operation, management, and protection of COMSEC material; and

- Facilitate the exchange of COMSEC information and CRO training among B/IOs.

d. Other requirements are as follows:

- Only NSA-approved COMSEC products and services must be used to secure classified information.

- USAID must acquire COMSEC products and services through and by methods approved by the service provider who serves as the centralized COMSEC acquisition authority.

552.3.20.2 Communication Security (COMSEC Operations)

Effective Date: 09/26/2017

COMSEC Operations must ensure:

- Telecommunication equipment is coordinated through the service provider.

- Communications occur via current NSA-approved encryption devices.

- COMSEC encryption devices adhere to the following:

  - Must be secured either in a server/encryptor room or in a GSA-approved

security container and an operational, alarm-capable Intrusion Detection System (IDS);

- The encryptor must be secured in an approved security container if it remains keyed within an unattended area;

- The encryptor must be secured in an approved security container if any individual without “Crypto Access for Use” has unescorted access to the devices;

- If a security container is not required, the Cryptographic Ignition Key (CIK) must be removed from the encryptor at close of business (COB) and stored in a GSA-approved security container;

- Currently approved GSA safes are required for the protection of the keying material during non-business hours; and

    - Physical and logical access to cryptographic information, equipment, and devices must remain limited only to COMSEC personnel who are formally appointed in writing and who are explicitly responsible for COMSEC and are actively enrolled in a Cryptographic Access Program; no exceptions (see **552.4**).

552.3.20.3 COMSEC Procedures
Effective Date: 09/26/2017

COMSEC procedures are as follows:

- COMSEC custodians must follow USAID and the service provider’s defined procedures; and

- Formal requests for COMSEC products and services, configurations, troubleshooting, or other concerns must be provided only to personnel who are involved with COMSEC operations.

552.3.21 Secure Voice, Video, and Fax
Effective Date: 09/26/2017

The purpose of this section is to provide USAID policy on secure voice, video, and fax communications. This section includes USAID baseline policy and standards for classified conferences, briefings, communications, and teleconferences, as well as secure video sessions, conversations and meetings in approved workspaces, and procurement of video and voice communication systems. This section also covers secure procurement and operation of equipment used to safeguard, protect, and process NSI, which requires, at a minimum, that products be procured, shipped, received, configured, tested, and placed into operations via “trusted” methods.

Security is designed to minimize the risk of unauthorized disclosure of NSI video, voice, and fax communications.

To achieve “trusted” procurement and implementation, USAID and the service provider must approve all hardware and software used to implement, enable, and accomplish NSI. Where and when required, the Classified Support team must implement TEMPEST certified equipment.

Classified video, telephone, and fax communications must adhere to service provider policies, standards, processes, and procedures.

Classified conversations must never happen over speaker phones. All end-user conferencing devices must have disabled classified (secure mode) speaker capability. Where possible, end-user voice devices must be installed and configured to operate only in secure mode by push-to-talk technologies. Noncompliance or altering/configuring push-to-talk mechanisms in open-microphone position must result in immediate removal of voice devices, documented counseling, and administrative and/or appropriate punitive penalty without exception.

Note: This does not include secure video or classified conference rooms where (and when) these rooms/areas are accredited, configured, authorized, and approved for speaker-enabled operations.

552.4 MANDATORY REFERENCES

552.4.1 External Mandatory References

Effective Date: 09/26/2017

Please note that some of the following links can only be accessed in Internet Explorer.

a. **18 FR 2489, 3 CFR, 1949-1953**

b. **CNSSD-500, Information Assurance (IA) Education, Training, and Awareness, August 2006**

c. **CNSSD-502, National Directive On Security of National Security Systems, December 16 2004**

d. **CNSSD-506, National Directive to Implement Public Key Infrastructure for the Protection of Systems Operating on Secret Level Networks, October 9, 2012**

e. **CNSSD-900, Governing Procedures of the Committee on National Security Systems (CNSS), September 21, 2012**

f. **CNSSD-901, National Security Telecommunications and Information Systems**

Security (CNSS) Issuance System, September 21, 2012

g. CNSSP-1, National Policy for Safeguarding and Control of Communications Security Material, September 2004

h. CNSSP-3, National Policy for Granting Access to U.S. Classified Cryptographic Information, October 2007

i. CNSSP-14, National Policy Governing the Release of Information Assurance (IA) Products and Services to Authorized U.S. Persons or Activities that are Not a Part of the Federal Government, November 2002

j. CNSSP-15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems, October 2012

k. CNSSP-17, Policy on Wireless Communications: Protecting National Security Information, May 2010

l. CNSSP-18, National Policy on Classified Information Spillage, June 2006

m. CNSSP-19, "National Policy Governing the Use of High Assurance Internet Protocol Encryptor (HAIPE) Products," February 2007

n. CNSSP-21, National Information Assurance Policy on Enterprise Architectures for National Security Systems, March 2007

o. CNSSP-22, Information Assurance Risk Management Policy for National Security Systems, January 2010

p. CNSSP-24, Policy on Assured Information Sharing (AIS) for National Security Systems (NSS), May 2010

q. CNSSP-25, National Policy For Public Key Infrastructure in National Security Systems, March 2009

r. CNSSP-26, National Policy on Reducing the Risk of Removable Media, November 2010: This document is designated FOUO. To access protected FOUO content in the CNSS Library, you must login with a Federal/DoD Public Key Infrastructure (PKI), Personal Identity Verification (PIV) or Common Access Card (CAC) client certificate correctly installed in your browser and click on the "CAC/PKI/PIV Login" button.

s. DOD 8570.01-M, Information Assurance Workforce Improvement Program, December 19, 2005, Incorporating Change 3, January 24, 2012

t. EO 9397, Relating to Federal Agency Use of Social Security Numbers, as Amended

u. EO 10450, Security Requirements for Government Employment, as Amended

v. EO 12333, United States Intelligence Activities, as amended

w. EO 12885, Amendment To Executive Order No. 12829

x. EO 12968, Access to Classified Information

y. EO 13011, Federal Information Technology, July 16, 1996 (Authority)

z. EO 13064, Further Amendment to EO 13010, Critical Infrastructure Protection

aa. EO 13292, Further Amendment to EO 12958, Classified National Security Information

ab. EO 13381, Strengthening Processes Relating To Determining Eligibility for Access to Classified National Security Information

ac. EO 13434, National Security Professional Development

ad. EO 13467, Reforming Processes Related To Suitability For Government Employment, Fitness For Contractor Employees, and Eligibility For Access To Classified National Security Information

ae. EO 13526, Classified National Security Information

af. EO 13556, Controlled Unclassified Information

ag. EO 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information

ah. Federal Information Security Management Act of 2002

ai. Federal Information Security Amendments Act of 2014

aj. ICD 705, Sensitive Compartmented Information Facilities, May 26 2010

ak. ICS 705-1, Physical and Technical Standards for Sensitive Compartmented Information Facilities, December 17, 2010

al. ICS 705-2, Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities, December 17, 2010

am. IC Tech Spec-For ICD/ICS 705 Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, version 1.2

an. National Security Act of 1947, as amended, 50 USC, 401 *et seq.*

ao. NIST Special Publications 800 Series

ap. NSTISSD-501, National Training Program for Information Systems Security (INFOSEC) Professionals, November 16, 1992

aq. NSTISSI No. 7003, December 13, 1996

ar. NSTISSP-11, Fact Sheet for the National Information Assurance Acquisition Policy, July 2003

as. NSTISSP-101, National Policy on Securing Voice Communications, September 14, 1999

at. NSTISSP-200, National Policy on Controlled Access Protection, July 15, 1987

au. Pub. L. 99-474, The Computer Fraud and Abuse Act

av. TSG Standard 1, Introduction to Telephone Security, March 1990

552.4.2 Internal Mandatory References

Effective Date: 09/26/2017

a. ADS 530, Emergency Planning Overseas

b. ADS 531, Continuity of Operations Program

c. ADS 545, Information Systems Security

d. ADS 549, Telecommunications Management

e. ADS 561, Security Responsibilities

f. ADS 565, Physical Security Programs (Domestic)

g. ADS 566, Personnel Security Investigations and Clearances

h. ADS 568, National Security Information Program

i. ADS 569, Counterintelligence Program

j. Classified Mandatory References

k. M/CIO Rules & Regulations

552.4.3 Mandatory Forms
Effective Date: 09/26/2017

a. DD Form 2875, System Authorization and Access Request (SAAR)

b. SF-312, Nondisclosure Agreement

c. SF-701, Activity Security Checklist

d. SF-702, Security Container Checklist

e. USAID Form 552-1, Classified Processing Compliance Review

f. USAID Form 552-2, Classified Information System User Agreement

g. USAID Form 552-3, Classified Spillage Questionnaire

h. USAID Visitor Register Log

552.5 ADDITIONAL HELP
Effective Date: 09/26/2017

a. 12 FAM 600, Information Security Technology

b. 12 FAM 610, Organization and Purpose of Computer Security (COMPUSEC)

c. 12 FAM 630, Department Security Configuration Guidelines

d. Department of State's Foreign Affairs Handbook

e. SEC Office of Security Web Page: Counterterrorism and Information Security

f. USAID Protective Distribution Policy (PDS)

552.6 DEFINITIONS
Effective Date: 09/26/2017

For additional definitions, please see the ADS Glossary.

access point (AP)
A location to connect to a device or network. (**Chapter 552**)

actor

An individual responsible for insider betrayals can be labeled as one or more of three different types of actors: 1) psychologically-impaired disgruntled or alienated employees; 2) ideological or religious radicals; and 3) criminals. Moreover, insiders are very often identifiable by more than one of these categories. (**Chapter 552**)

Administrative Management Staff (AMS)
The Administrative Management Staff (GC/AMS) reviews internal office operations and provides management, administrative, and logistic support to all elements of GC. GC/AMS manages the office's OE budget and FTEs and provides services for travel, space planning, administrative procurement, and reproduction and printing services. The staff develops recruitment requirements, recommends selections, and represents GC in the personnel decision-making process. GC/AMS administers the automation program and develops and maintains the GC law library. (**Chapter 552**)

approved
Formally reviewed and certified as meeting acceptable technical, operational and security baseline compliance (see “authorized”). (**Chapter 552**)

approving official (AO)
Formerly designated as the “Designated Accrediting Authority” (AO), the official with the authority to assume formal responsibility for operating information systems at an acceptable level of risk. (**Chapter 552**)

authorized
Formally accepted as an approved and deployable technology within the IT enterprise (see “approved”). (**Chapter 552**)

Bluetooth technology
A specification for low-cost, wireless communication and networking between PCs, mobile phones, PDAs, and other portable devices. (**Chapter 552**)

Bureau/Independent Office (B/IO)
Inclusive of any USAID Bureau or Office, with approved authority to engage in or perform classified activities. (**Chapter 552**)

Chief Information Security Officer (CISO)
CISO operates in four primary capacities: 1) Define the security and privacy requirements with which IT systems and telecommunications must comply, based on federal mandates and legislative requirements; 2) Monitor systems and projects in development to validate that system security and electronic records privacy complies with established guidance, including that Agency employees are trained in information systems security; 3) Detect and respond to information systems incidents; and 4) Perform computer forensics investigations.

Specifically, the CISO is responsible for security policy and implementation oversight; developing IT security policy; promoting enterprise security technologies and best

practices; implementing and managing security and intrusion detection tools; and monitoring and evaluating security performance. CISO is also responsible for information systems security incident management and response, including detecting, reporting, and responding to security incidents. The CISO performs these same functions in the area of COMSEC within the Agency.

The CISO interacts directly with Mission and B/IO managers and systems administrators in monitoring security performance and advising on resolution of identified problems. (**Chapter 552**)

classified activity
Any approved and authorized combined or single classified activity associated with national security information (NSI), NSI systems or NSI resources (discuss, process, transmit video, teleconference, media handling use and/or storage). (**Chapter 552**)

classified processing
Computing, processing, discussing, and reviewing physical documents or media, conversation, video, video-teleconference, teleconference, telephone conversations, or any other combination of classified operations. (**Chapter 552**)

classified spaces/workspaces
Refers to any authorized area, room, office, workspace, or facility where classified activities do, or may occur within USAID, the term is synonymous with “Restricted Space.” (**Chapter 552**)

close of business (COB)
The end of the business day. (**Chapter 552**)

communications security (COMSEC)
Discipline of preventing unauthorized interceptors from accessing telecommunications in an intelligible form, while still delivering content to the intended recipients. In the United States Government culture, it is often referred to by the abbreviation ‘COMSEC’. The field includes cryptographic security, transmission security, emission security, traffic-flow security and physical security of COMSEC equipment. COMSEC is used to protect both classified and unclassified traffic on government networks, including voice, video, and data. It is used for both analog and digital applications, and both wired and wireless links. (**Chapter 552**)

communication security (COMSEC) material control system (CMCS)
COMSEC refers to communication security. This consists of all steps taken to protect information of value when it is being communicated. COMSEC has four main components: transmission security, physical security, emission security, and cryptographic security.

Transmission security is that component of COMSEC which is designed to protect transmissions from unauthorized intercept, traffic analysis, imitative deception and

disruption. CMCS refers specifically to the procedural safeguards placed on COMSEC equipment and materials, covering every phase of their existence from creation through disposition, and are designed to reduce or eliminate the possibility of such compromise. (**Chapter 552**)

Communications Security (COMSEC) Office of Record (COR)
The parent owner or COMSEC service provider of child or sub COMSEC account holders. (**Chapter 552**)

Communications Security (COMSEC) Responsible Officers (CROs)
CROs are formally appointed and trained B/IO personnel who, in coordination with the Agency COMSEC custodian(s), provide direct B/IO COMSEC security support and requirements. (**Chapter 552**)

Communications Security (COMSEC) Utility Program (CUP)
The Communications Security Program is a pool of selected information assurance (IA) security equipment available to federal departments and agencies on a reimbursable or temporary basis, used to satisfy crisis, contingency, and emergent national security requirements. (**Chapter 552**)

Continental United States (CONUS)
A term referring to the contiguous United States. They include the 48 U.S. states on the continent of North America south of Canada and north of Mexico, plus the District of Columbia. The term excludes the states of Alaska and Hawaii, and all off-shore U.S. territories and possessions, such as Puerto Rico. (**Chapter 552**)

Contracting Officer (CO)
A person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings. The term includes certain authorized representatives of the contracting officer acting within the limits of their authority as delegated by the contracting officer. A single contracting officer may be responsible for duties in any or all of these areas. (**Chapter 552**)

Contracting Officer's Representative (COR)
Also formally known as the COTR, the COR serves as the technical liaison between the Contracting Officer (CO) and the contractor. The COR gives technical directions/guidance to the contractor, receives and inspects completed services or supplies upon delivery, monitors government-furnished property, approves the contractor's requests for payment, and performs any other delegated duties that would otherwise be the responsibility of the CO. (**Chapter 552**)

controlled cryptographic items (CCIs)
A U.S. National Security Agency term for secure telecommunications or information handling equipment, associated cryptographic component, or other hardware item which performs a critical COMSEC function. Items so designated may be unclassified but are subject to special accounting controls and required markings. (**Chapter 552**)

Cryptographic Ignition Key (CIK)
A physical (usually electronic) token used to store, transport, and protect cryptographic keys and activation data. (**Chapter 552**)

cyber forensics
Cyber forensics, also called computer forensics or digital forensics, is the process of extracting information and data from computers to serve as digital evidence for civil purposes or, in many cases, to prove and legally prosecute cyber-crime. (**Chapter 552**)

Defense Information Security Agency (DISA)
A United States Department of Defense agency that provides IT and communications support to the President, Vice President, Secretary of Defense, the military services, and the Combatant Commands. (**Chapter 552**)

Department of the Army (DA)
One of the three military departments within the Department of Defense, subject to the limits of the law, and the direction of the Secretary of Defense and the President. (**Chapter 552**)

Department of the Navy (DON)
A military department within the Department of Defense, subject to limits of the law, and the direction of the Secretary of Defense and the President. (**Chapter 552**)

disposition
Act of disposing; transferring to the care or possession of another. (**Chapter 552**)

employee
Employee includes all USAID U.S. citizen direct-hire personnel and personal service contractors. This chapter uses the term employee to mean anyone who is certified and/or authorized access to classified information by virtue of a contract, consulting agreement, detail, grant, appointment to an advisory panel, or who is otherwise authorized access to classified systems or information. Access includes NSI resources at USAID facilities, regardless of the media, network classification or employment category. (**Chapter 552**)

entry on duty (EOD)
First day of employment. (**Chapter 552**)

Federal Information Security Management Act (FISMA)
(44 USC § 3541, *et seq*.), a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub. L. 107-347, 116 Stat. 2899). The act recognizes the importance of information systems security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information systems security for the information and information systems that support the operations and

assets of the agency, including those provided or managed by another agency, contractor, or other source. (**Chapter 545** and **552**)

General Services Administration (GSA)
An independent agency of the United States Government, established in 1949 to help manage and support the basic functioning of federal agencies. The GSA supplies products and communications for U.S. Government offices, provides transportation and office space to federal employees, and develops government-wide, cost-minimizing policies and other management tasks. (**Chapter 552**)

government-furnished equipment (GFE)
According to the Federal Acquisition Regulation (FAR) at 45.101, a tangible item that is functionally complete for its intended purpose, durable, nonexpendable, and needed for performance of a contract. Equipment is not intended for sale, and does not ordinarily lose its identity or become a component part of another article when put into use. Equipment does not include material, real property, special test equipment or special tooling. (**Chapter 552**)

government-off-the-shelf (GOTS)
A FAR term defining software and hardware government products which are ready-to-use. They were created and are owned by the government. Typically GOTS are developed by the technical staff of the government agency for which it is created. It is sometimes developed by an external entity, but with funding and specification from the agency. Because agencies can directly control all aspects of GOTS products, these are generally preferred for government purposes. GOTS software solutions can normally be shared among federal agencies without additional cost. GOTS hardware solutions are typically provided at cost. (**Chapter 552**)

information system (IS)
The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, and dissemination of information. This term includes both automated and manual information systems. (Source: NSTISSI 4009) (**Chapters 550**, **552**, and **620**)

Information System Security Manager (ISSM)
The security official responsible for the IS security program for a specific directorate, office, or contractor facility. (**Chapter 552**)

incident detection (ID)
The recognition of a threat or a potential threat to a system or network. An incident can be detected by a sensor, a network analyst, or a user. (**Chapter 552**)

incident response (IR)
The reaction to an incident. It involves tracking and documenting the incident, reporting, measuring, identifying and stopping incident effects, and adding or improving security controls to prevent future incidents of the type. (**Chapter 552**)

Information Security Oversight Office (ISOO)
Oversees the security classification programs in both government and industry and reports annually to the President on their status. They monitor approximately 65 executive branch departments, independent agencies and offices, and their major components. (**Chapter 552** and **568**)

information systems security (ISS)
For purposes of this chapter, ISS is the protection afforded to information and telecommunications systems, which process classified national security-related information in order to prevent exploitation through intentional or unintentional disclosure, interception, unauthorized electronic access, or related technical intelligence threats. (**Chapter 552**)

Information Systems Security Officer (CIO ISSO)
Individual responsible to the senior agency information systems security officer, authorizing official, or information system owner for ensuring the appropriate operational security posture is maintained for an information system or program. (**Chapter 552**)

information technology (IT)
The development, management, and use of computer-based information systems. (**Chapter 552**)

Information Technology Configuration Control Board (ITCCB)
The ITCCB is established under the authority of the CIO. It is the governing authority for controlling the technical baselines for USAID IT projects and operations. It reviews, approves, disapproves, and defers changes to baselines under the management of M/CIO. In addition, it oversees change control processes, and evaluates change requests and implementation of approved changes. (**Chapter 552**)

Institute of Electronics and Electrical Engineers (IEEE)
A scientific and educational institute directed toward the advancement of the theory and practice of electrical, electronics, communications and computer engineering, as well as computer science, the allied branches of engineering and the related arts and sciences. A publisher of scientific journals, the institute is a leading standards development organization for the development of industrial standards in a broad range of disciplines, including electric power and energy, biomedical technology and healthcare, information technology, information assurance, telecommunications, consumer electronics, transportation, aerospace, and nanotech. (**Chapter 552**)

laptop
A type of portable electronic device (PED), usually a traditional notebook computer with a folding screen, with features similar to a standard desktop computer such as internal hard drive, standard communications and peripheral data ports, and larger in size than other PEDs. (**Chapter 552**)

Level of Effort (LOE)
In project management, work of a general or supportive nature (such as coordination, follow up, liaison) that does not result in a definitive end product or outcome. (**Chapter 552**)

Media Access Control (MAC)
A protocol that is a sublayer of the data link layer 2. The MAC sublayer provides addressing and channel access control mechanisms which enable several terminals or network nodes to communicate within a multiple access network that incorporates a shared medium, e.g. Ethernet. The hardware that implements the MAC is referred to as a medium access controller. The MAC sublayer acts as an interface between the logical link control (LLC) sublayer and the network's physical layer. The MAC layer emulates a full-duplex logical communication channel in a multi-point network. This channel may provide unicast, multicast or broadcast communication service. (**Chapter 552**)

Memorandum of Agreement (MOA)
A document outlining the cooperative terms, responsibilities, and often funding of two entities to work in partnership on certain listed projects. The agreed responsibilities of the partners must be listed and the benefits of each party must be listed. (**Chapter 545** and **552**)

Memorandum of Understanding (MOU)
A document describing a bilateral or multilateral agreement between parties. It expresses a convergence of will between the parties, indicating an intended common line of action. It is often used in cases where parties either do not imply a legal commitment or in situations where the parties cannot create a legally enforceable agreement. In some cases depending on the exact wording, MOU can have the binding power of a contract. Whether or not a document constitutes a binding contract depends only on the presence or absence of well-defined legal elements in the text proper of the document (the so-called "four corners"). The required elements are: offer, consideration, and acceptance. (**Chapter 552**)

multi-function device (MFD)
A single device that has the capability to perform multiple functions such as voice and video/photo recording, infrared (IR), and video/photo or text storage and wireless transmissions. (**Chapter 552**)

National Capital Region (NCR)
The National Capital Region (NCR), headquartered in Washington, DC, administers the National Mall and monumental core parks that were established the same time the Nation's Capital was founded in 1792.These oldest national park areas, along with dozens of historic sites, natural areas and Civil War battlefields comprise today's National Capital Region of the National Park Service. (**Chapter 552**)

National Institute of Standards and Technology (NIST)
A non-regulatory federal agency within the U.S. Department of Commerce. The NIST

mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. (**Chapter 545** and **552**)

National Security Agency (NSA)
A cryptologic intelligence agency of the United States Department of Defense responsible for the collection and analysis of foreign communications and foreign signals intelligence, as well as protecting U.S. Government communications and information systems. This involves information systems security and cryptanalysis/cryptography. (**Chapter 545** and **552**)

National Security Information (NSI)
Information which, if disclosed to unauthorized entities or personnel, has potential to, and could reasonably be expected to cause damage to the national security. (**Chapter 552**)

Nondisclosure Agreement (NDA)
A legal contract between two parties which outlines confidential materials the parties wish to share with one another for certain purposes, but wish to restrict from generalized use. (**Chapter 545** and **552**)

open storage (OS)
The storage of classified material within an approved and accredited classified processing workspace in any configuration other than within GSA-approved security containers. (**Chapter 552**)

optional form (OF)
Government form used for various purposes. (**Chapter 552**)

Personal Digital Assistant (PDA)
A hand-held device that is a type of portable electronic device (PED) used for computing and information storage and retrieval capabilities such as calendars and address books. Some examples include Palm Pilots, iPhone or Android devices, and MP3 players. (**Chapter 552**)

personal identification number (PIN)
A personal identification number (PIN, pronounced “pin”; often erroneously PIN number) is a secret numeric password shared between a user and a system that can be used to authenticate the user to the system. Typically, the user is required to provide a non-confidential user identifier or token (the user ID) and a confidential PIN to gain access to the system. Upon receiving the user ID and PIN, the system looks up the PIN based upon the user ID and compares the looked-up PIN with the received PIN. The user is granted access only when the number entered matches with the number stored in the system. Hence, despite the name, a PIN does not personally identify the user. (**Chapter 552**)

personally owned devices/equipment
Equipment that is not owned or leased by the Federal Government, or operated by a contractor on behalf of the Federal Government. (**Chapter 552**)

personnel
Any person, in any capacity, who include, but are not limited to, direct-hires, licensees, or any person, group or representative, operating or functioning in any role in support of or on behalf of, or in a capacity that represents USAID, that creates, generates, accesses, processes, distributes, discusses, views, manipulates, transmits, communicates and/or provides security or NSI system support in any manner, by any means (physical, technical or logical). (**Chapter 552**)

plan of action and milestones (POA&M)
According to OMB M-02-01, a POA&M identifies tasks to do. It details resources to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. A POA&M assists agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. (**Chapter 545** and **552**)

Point of Contact (POC)
A person or business unit serving as the focal point associated with identified resources. POCs are used in many cases where information is time-sensitive and accuracy is important. (**Chapter 552**)

portable (or personal) electronic device (PED)
Any non-stationary (government or non-government owned) electronic apparatus with singular or multiple capabilities of recording, storing, processing, and/or transmitting data, video/photo images, and/or voice emanations. This definition generally includes, but is not limited to, laptops, PDAs, pocket PCs, palmtops, media players (MP3s), memory sticks (thumb drives), cellular telephones, PEDs with cellular phone capability, pagers, and Play station (and similar technologies). Use of personal devices to conduct official Agency business is prohibited outside of extreme circumstances outlined in ADS Chapter **502** and **545**. (**Chapter 552**)

protective distribution system (PDS)
A fiber-optics telecommunication system that includes terminals and adequate acoustical, electrical, electromagnetic, and physical safeguards to permit its use for the unencrypted transmission of classified information. (**Chapter 552**)

Public Key Infrastructure (PKI)
A set of hardware, software, people, policies, and procedures which create, manage, distribute, use, store, and revoke digital certificates. In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority. (**Chapter 545** and **552**)

radio frequency (RF)

Radio frequency (RF) is a rate of oscillation in the range of about 3 kHz to 300 GHz, which corresponds to the frequency of radio waves, and the alternating currents which carry radio signals. RF usually refers to electrical rather than mechanical oscillations, although mechanical RF systems do exist (see mechanical filter and RF MEMS). (**Chapter 552**)

radio frequency identification (RFID)
The use of a wireless non-contact system employing radio-frequency electromagnetic fields to transfer data from a tag attached to an object for the purposes of automatic identification and tracking. (**Chapter 545** and **552**)

regulatory governance
Includes all applicable, relevant and current final version federal mandates (e.g., EOs, CNSS, National Institute of Standards and Technology (NIST), Federal Information Systems Management Act (FISMA), and any applicable others). (**Chapter 552**)

restricted space
Areas formally approved and authorized for classified activities that consist of closed storage, open storage, Secure Compartmented Information Facility (SCIF), Independent Office, Bureau, conference room, workspace or work area. (**Chapter 552**)

rules of behavior (ROB)
Rules that clearly delineate responsibilities and expected behavior of all individuals with access to a system. (**Chapter 545** and **552**)

secure compartmentalized facility (SCIF)
An enclosed area within a building used to process Sensitive Compartmented Information (SCI)-level classified information. (**Chapter 552**)

secure compartmentalized information (SCI)
SCI is classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence. (**Chapter 552**)

secure video-teleconference (SVTC)
The conduct of a videoconference by a set of telecommunication technologies. They allow two or more locations to communicate by simultaneous two-way video and audio transmissions. Security protects the video-teleconference against danger, damage, loss, or crime. (**Chapter 552**)

Security Assessment and Authorization (SA&A)
Certification is the comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. Source: NSTISSI No. 1000. (**Chapter 552**)

Security accreditation is the official management decision given by a Designated Approving Authority (AO) to authorize operation of an information system, and to explicitly accept the risk to Agency operations, Agency assets, or individuals based upon the agreed upon implementation of a prescribed set of security controls. (**Chapter 552**)

Sensitive Compartmented Information Facility (SCIF)
A SCIF is an accredited area, room, group of rooms, buildings, or installation where SCI (sensitive compartmented information) may be stored, used, discussed, and/or electronically processed. SCIFs will be afforded personnel access control to preclude entry by unauthorized personnel. (**Chapter 552**)

service level agreement (SLA)
Also called service level contract. A contract between a service provider and a customer, it details the nature, quality, and scope of the service to be provided. In practice, the term SLA is sometimes used to refer to the contracted delivery time (of the service) or performance. (**Chapter 552**)

service provider (SP)
Applicable policy and baseline requirements of any entity (internal (e.g., M/CIO, SEC, CIO ISSO); outsourced, third party provider, etc.) that provides classified products, services and/or support to USAID users, facilities, and workspaces. (**Chapter 552**)

standard operating procedure (SOP)
A written document providing a set of steps designed to produce a defined outcome. (**Chapter 552**)

System Authorization Access Request (SAAR)
DD Form 2875, a form used pursuant to EOs 9397, 10450; and Pub. L. 99-474, the Computer Fraud and Abuse Act. This is used to record names, signatures, and other identifiers to validate the trustworthiness of individuals requesting access to systems and information. Records may be electronic and/or paper. SAARs can be agency specific, or from existing resources, as long as minimum information is captured (**Chapter 552**)

system security plan (SSP)
An overview of the security requirements of the computer system and the controls in place or planned to meet those requirements. The SSP delineates responsibilities and expected behavior of all individuals who access the computer system. (**Chapter 545** and **552**)

TEMPEST
The vulnerabilities of compromising emanations from communications and other electrical equipment that contain data. Requirements are set out in document NACSIM 5100A, which is classified. (**Chapter 552**)

TEMPEST countermeasures (Telecommunications Electronics Material Protected from Emanating Spurious Transmissions)
This term refers to technologies involving the monitoring (and shielding) of devices that emit electromagnetic radiation (EMR) in a manner that can be used to reconstruct intelligible data. Requirements are set out in document NACSIM 5100A, which is classified. (**Chapter 552**)

Underwriters Laboratories (UL)
A safety consulting and certification company that provides safety-related certification, validation, testing, inspection, auditing, advising, and training. (**Chapter 552**)

upward adjustment (UA)
A document increasing the amount of a previously recorded obligation when the actual amount is larger than the estimated amount. An upward adjustment may require an amendment to the original obligating document. (**Chapter 552**)

user
Any government employees in any hire and/or support capacity. (**Chapter 552**)

user identifications (IDs)
User IDs, also known as logins, user names, logons, or accounts, are unique personal identifiers for agents of a computer program or network that is accessible by more than one agent. These identifiers are based on short strings of alphanumeric characters, and are either assigned or chosen by the users. (**Chapter 552**)

Visitation Access Requests (VARs)
Formal vetting and approval for access requests to facilities, installations, systems, or spaces by non-Agency employees. (**Chapter 552**)

visitors/guests
Any non-USAID employee, or any USAID employee, not currently assigned to USAID Washington, or one of its National Capital Region (NCR) duty locations. (**Chapter 552**)

Washington (W)
USAID facilities in the Washington region. (**Chapter 552**)

wireless technologies
Wireless communication is the transfer of information between two or more points that are not connected by an electrical conductor. The most common wireless technologies use electromagnetic wireless telecommunications, such as radio. With radio waves distances can be short, such as a few meters for television or as far as thousands or even millions of kilometers for deep-space radio communications. It encompasses various types of fixed, mobile, and portable applications, including two-way radios, cellular telephones, personal digital assistants (PDAs), and wireless networking. Other examples of applications of radio wireless technology include GPS units, garage

door openers, wireless computer mice, keyboards and headsets, headphones, radio receivers, satellite television, broadcast television and cordless telephones. Less common methods of achieving wireless communications include the use of light, sound, magnetic, or electric fields, and hearing or visual impairment aids. (**Chapter 552**)

552_092617