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
The transfer, retirement, and/or disposal of records or non-record material. (**Chapter 158, 502, 552, 536**)

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**)

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 system
A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.] Source: NIST: Key Glossary of Information Security Terms. (**Chapter 502, 508, 509, 545, 550, 552, 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**)

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)
As defined in M-15-14: Management and Oversight of Federal Information Technology Resources, Information technology includes:

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

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

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

services that support any point of the lifecycle of the equipment or service), and related resources.

d. The term "information technology" does not include any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment.

(**Chapters 300**, **518**, **519**, **541**, **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)
Documents 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 will be listed and the benefits of each party will be listed. (**Chapter 545, 552**)

Memorandum of Understanding (MOU)
A document that sets forth a set of intentions between participants. MOUs are generally designed as non-binding instruments and establish political (not legal) commitments. (**Chapter 201, 545, 552**)

Mobile Device
Mobile devices include, but are not limited to, any portable electronic device capable of transmitting, receiving, and/or intercepting wireless or Bluetooth signals and/or capable of capturing, transmitting, and/or intercepting audio, voice and/or devices that run on "a self-contained power source" including: electronic readers; portable computers such as notebooks, laptops, and tablets that are Non-Government Furnished Equipment (N-GFE) (*e.g.,* devices not provided by USAID or visitor devices); smart watches; communications devices: cellular or Bluetooth devices, audio/video/data recording or playback devices, remote sensors, messaging devices, two-way radios, and two-way (transmit/receive) electronic devices; Personal Digital Assistants (PDAs); pagers; health and fitness trackers; Near Field Communication; wireless technology; and wireless gaming systems. **(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
A room or area constructed for the purpose of safeguarding national security information that, because of its size or nature, or operational necessity, cannot be adequately protected by the normal safeguards or stored during nonworking hours in approved containers. Open storage rooms permit classified information to be outside of a GSA-approved container when not within one's direct personal control. (**Chapter 552, 568**)

optional form
A form developed by a Federal agency for use in two or more agencies and approved by the General Services Administration (GSA) for non-mandatory government-wide use. Carries an OF form number. (**Chapter 505, 552**)

Personal Digital Assistants (PDAs)
This is a term for any small mobile handheld device that provides computing and information storage and retrieval capabilities. A PDA is a Mobile Computing Device (MCD). (**Chapter 545, 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
The number of complete alternating electrical currents. The unit of frequency measurement is the hertz (Hz) and is one cycle per second. Radio frequencies fall

between 3 KHz and 30 GHz and the radio spectrum is divided into eight frequency bands:

Frequency	Classification	Designation
3 to 30 KHz	Very low frequency	VLF
30 to 300 KHz	Low Frequency	LF
300 to 3000 KHz	Medium frequency	MF
3 to 30 MHz	High frequency	HF
30 to 300 MHz	Very high frequency	VHF
300 to 3000 MHz	Ultra high frequency	UHF
3 to 30 GHz	Super high frequency	SHF
30 to 300 GHz	Extremely high frequency	EHF

(**Chapter 552, 564**)

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
An area where storage, processing, discussions, and handling of classified documents is authorized. (**Chapter 517, 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. 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
To increase the amount of a previously recorded obligation when the actual amount is determined and it is larger than the estimated amount. An upward adjustment may require an amendment to the original obligating document. (**Chapter 552, 621**)

user
All persons authorized to access and use the USAID network and the systems supported by it. Users have received favorable employment eligibility status or have successfully passed a background check or investigation. A user can also be someone who uses information processed by USAID‘s information systems and may have no access to USAID‘s information systems. Users are the only subclass that cannot possess elevated privileges. (**Chapter 545, 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**)

visitor
An individual, who is not authorized to access the USAID facility, to which they have gained access, and who is being escorted by an authorized individual. (**Chapter 545, 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_011321