12 FAM 090

DEFINITIONS OF DIPLOMATIC SECURITY TERMS

(CT:DS-207; 04-03-2014)
(Office of Origin: DS/MGT/PPD)

12 FAM 091 TERMS

(CT:DS-207; 04-03-2014)

A

Access: *The approved ability and the means necessary to make use of information; controlled physical facilities; and/or information systems.*

Access control: *The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).*

ACR: Abbreviation for acoustic conference room, an enclosure that provides acoustic but not electromagnetic emanations shielding; ACRs are no longer procured; treated conference rooms (TCRs) are systematically replacing them.

Advisory sensitivity attributes: User-supplied indicators of file sensitivity that alert other users to the sensitivity of a file, to handle it appropriate to its defined sensitivity. Advisory sensitivity attributes are not used by the automated information system (AIS) to enforce file access controls in an automated manner.

Agency: A Federal agency including department, agency, commission, etc., as defined in 5 U.S.C. 552(e).

Application system: *A software program that performs a specific function directly for a user and may be executed without access to system control, monitoring, or administrative privileges.*

Application system owner: *A person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an application system.*

Areas to be accessed: Embassy areas to be accessed are defined in two ways. Controlled access areas (CAAs) are spaces where classified operations/discussions/storage may occur. *Non-controlled* access areas are spaces where classified operations/discussions/storage do not occur.

Audit log: *A chronological record of system activities. Includes records of system accesses and operations performed in a given period.*

Audit trail: *A record showing who has accessed an Information Technology (IT) System and what operations the user has performed during a given period.*

Authenticate: *To verify the identity of a user, user device, or other entity; and the integrity of data.*

***Authentication**: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.*

***Authenticator**: The means used to confirm the identity of a user, processor, or device (e.g., user password or token). (Also, see Multi-factor Authentication).*

***Authenticity**: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.*

***Authorization**: Access privileges granted to a user, program, or process.*

***Authorization boundary:** All components of an information system to be authorized for operation by an authorizing official, and excludes separately authorized systems to which the information system is connected.*

Authorized access list: A list developed and maintained by the information systems security officer or personnel who are authorized unescorted access to the computer room.

Automated information system (AIS): An assembly of hardware, software, and firmware used to electronically input, process, store, and/or output data. Examples include: mainframes, servers, desktop workstations, *thin clients*, and mobile devices (e.g., laptops, e-readers, smartphones, tablets) Typically, system components include, but are not limited to: central processing units (CPUs), monitors, printers, *switches, routers, media converters,* and removable storage media, such as flash drives. An AIS may also include nontraditional peripheral equipment, such as networked digital copiers, and cameras and audio recording/playback devices used to transfer data to or from a computer. (NOTE: The Department's telework solution, e.g., one-time password generators, is an extension of the Department's AISs.)

***Availability**: Ensuring timely and reliable access to and use of information.*

B

***Backup**: Copy of files and programs made to facilitate recovery, if necessary.*

***Baseline configuration**: Consists of the minimum information system security and operational controls required for Department information systems.*

***Biometrics**: A measurable physical characteristic or personal behavioral trait*

used to recognize the identity, or verify the claimed identity of an applicant. Facial images, fingerprints, and iris scan samples are examples of biometrics.

Black: *Designation applied to encrypted information and the information systems, the associated areas, circuits, components, and equipment processing that information. See also RED.*

***Blacklisting**: The process used to identify: (i) software programs not authorized on an information system; or (ii) prohibited Universal Resource Locators (URL)/Web sites.*

***Breach**: See* 5 FAM 463.

Bluetooth: *A standard for short-range radio frequency (RF) communication used primarily to establish wireless personal area networks (WPANs).*

***Boundary protection**: Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).*

***Boundary protection device**: A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) provides information system boundary protection.*

Building passes: Those passes the Bureau of Diplomatic Security (DS) issues to permanent Department employees possessing a security clearance and a minimum of career-conditional status, and to DS-cleared contractors and other individuals (such as members of the press, or employee family members, etc.) with a legitimate need to enter Department facilities on a regular basis. Each pass has the holder's photograph, an individual identification number, expiration date, and may provide access through an electronically operated gate or other entrance. *See personal identity verification (PIV).*

Bulk Load Control Officer (BLCO): The BLCO is authorized to supervise the preparation of the container or pallet.

C

***CARDS**: Acronym for COMSEC Accounting and Reporting Distribution System, a name used to refer to the Comsec Material Control System (CMCS) utilized for COMSEC recordkeeping*.

"Carve-out" contract: A classified contract issued in conjunction with an approved Special Access Program (SAP) wherein the designated cognizant SAP security office retains inspection responsibility, in whole or in part. While the term carve-out technically only applies to the security function, it may also be used to designate contract administration services, audit, review, and other

functions performed by groups other than those who normally accomplish these tasks.

Central Office of Record (COR): The Department element that keeps records of accountable COMSEC material held by accounts subject to its oversight.

Classification: The determination that certain information requires protection against unauthorized disclosure in the interest of national security, coupled with the designation of the level of classification: Top Secret (TS), Secret, or Confidential.

Classification authority: *The original classification authority or derivative classifier described in the classification block by the individual's name or position who classified document. (See original classification authority.)*

Classification guides: Documents issued in an exercise of authority for original classification that include determinations with respect to the proper level and duration of classification of categories of classified information.

Classified Diplomatic Pouch: A properly documented and sealed envelope, parcel, shipping container, or any other kind of receptacle used by diplomatic missions to transmit approved correspondence, documents, publications, and other articles for official use between the Department, post, and between posts. Diplomatic pouches are protected under Article 27 of the *Vienna Convention on Diplomatic Relations* (see 12 FAM 111.2) from being searched, seized, or detained. Classified diplomatic pouches are prepared in accordance with 14 FAM and accompanied by appropriately cleared diplomatic couriers.

Classified information: Information or material, herein collectively termed information, owned by, produced for or by, or under the control of the U.S. Government, and that has been determined pursuant to Executive Order 13526 or prior orders to require protection against unauthorized disclosure, coupled with the designation of the level of classification.

***Classified information spillage**: When classified data is processed or received on an information system with a lower level of classification.*

Classifier: An individual who makes a classification determination and applies a security classification to information or material. A classifier may either be a classification authority or may assign a security classification based on a properly classified source or a classification guide.

Clear mode: Unencrypted plain text mode.

Cleared U.S. citizen: A citizen of the United States who has undergone a background investigation by an authorized U.S. Government Agency and been issued a Confidential, Secret, or Top Secret security clearance in accordance with Executive Orders 12968 and 10450 and implementing guidelines and standards published in 32 CFR 147. Abroad: Cleared U.S. citizens are required to have, at minimum, Secret-level clearances.

Code room: The designated and restricted area in which cryptographic

operations are conducted.

Collateral information: *A common reference to national security information, excluding national intelligence information, classified in accordance with* Executive Order 13526*, dated January 5, 2010.*

***Common carrier**: In a telecommunications context, a telecommunications company that holds itself out to the public for hire to provide communications transmission services. (NOTE: In the United States, such companies are subject to regulation by Federal and state regulatory commissions.)*

***Common criteria**: A Governing document created by the National Information Assurance Partnership (NIAP) that provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems.*

Communication protocols: A set of rules that govern the operation of hardware or software entities to achieve communication.

Communications security (COMSEC): The protection resulting from the proper application of physical, technical, transmission, and cryptologic countermeasures to a communications link, system, or component.

Communications system: A mix of telecommunications and/or automated information systems used to originate, control, process, encrypt, and transmit or receive information. Such a system generally consists of the following connected or connectable devices:

(1) Automated information equipment (AIS) on which information is originated;

(2) A central controller of, principally, access rights and information distribution;

(3) A telecommunications processor which prepares information for transmission; and

(4) National-level devices, which encrypt information (COMSEC/CRYPTO/CCI) prior to its transmission via Diplomatic Telecommunications Service (DTS) or commercial carrier.

Compromise: *Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.*

Compromising emanations: Intentional or unintentional intelligence-bearing signals which, if intercepted and analyzed, disclose national security information transmitted, received, handled, or otherwise processed by any information processing equipment. Compromising emanations consist of electrical or acoustical energy emitted from within equipment or systems (e.g.,

personal computers, workstations, facsimile machines, printers, copiers, and typewriters) which process national security information.

Computer Incident Response Team (CIRT): *The CIRT is the central reporting point for cybersecurity incidents within the Department. CIRT maintains 24x7 monitoring of network traffic for malicious and hostile security breaches and conducts security monitoring of the Department's unclassified and classified networks to ensure the integrity, availability, and confidentiality of the IT infrastructure. CIRT operations provide near real-time detection, collection, analysis, correlation, and reporting of cybersecurity events that pose an immediate threat to the Department's networks.*

***Computer room**: A computer room, also called a server room or data center, is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression), and security devices.*

***COMSEC**: Communications security.*

COMSEC account: The administrative entity, identified by an account number, used to maintain accountability, custody, and control of COMSEC material.

COMSEC custodian: *An individual designated by proper authority to be responsible for the receipt, transfer, accounting, safeguarding, and destruction of COMSEC material assigned to a COMSEC account. Only full-time Department personnel are eligible for appointment. If critical need, due to personnel shortage arises, a temporary waiver may be granted to appoint a contractor as an Alternate COMSEC Custodian.*

COMSEC facility: *An authorized and approved space used for generating, storing, repairing, or using COMSEC material*.

COMSEC material: *An item designed to secure or authenticate telecommunications. COMSEC material includes, but is not limited to key, equipment, devices, documents, firmware, or software that embodies or describes cryptographic logic and other items that perform COMSEC functions*.

COMSEC Material Control System (CMCS): *Logistics and accounting system through which COMSEC material marked "CRYPTO" is distributed, controlled, and safeguarded. Included are the COMSEC central offices of record, crypto logistic depots, and COMSEC accounts. COMSEC material other than key may be handled through the CMCS.*

COMSEC officer: The properly appointed individual responsible to ensure that COMSEC regulations and procedures are understood and adhered, the COMSEC facility is operated securely, that personnel are trained in proper COMSEC practices, and who advises on communications security matters*Only full-time Department direct-hire employees are eligible for appointment.*

Confidential-cleared U.S. citizen: A citizen of the United States who has undergone a background investigation by an authorized U.S. Government Agency and been issued a Confidential security clearance, in accordance with Executive Order 13526 and implementing guidelines and standards published in 32 CFR 147.

Confidentiality: *Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.*

Configuration control: *A method for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.*

Construction security certification: Certification/confirmation is required from the Department if any new construction or major renovation is undertaken in the controlled access area (CAA). A site security plan must be submitted prior to commencing work. The construction security of a new building or major renovation project (over $1 million) affecting CAAs or public access controls (PACs) must be certified to Congress. The construction security of projects less than $1 million affecting CAAs or PACs is certified internally within the Department.

Consumer electronics: Any electronic/electrical devices, either *Alternate Current (AC) or Direct Current (DC)* powered, which are not part of the facility infrastructure. Some examples are radios, televisions, electronic recording or playback equipment, PA systems, *and* paging devices.

Container: A cube shaped structure commonly referred to as a unit load device (ULD). It is primarily used for shipping classified diplomatic pouches via various modes of conveyance.

Containerize: The process of loading classified diplomatic pouches into an enclosed unit load device (ULD) (i.e., a container).

Control officer: Maintains chain of custody of the classified diplomatic pouch through signing for the classified diplomatic pouch on Form DS-7600.

Controlled access area: *Per 12 FAH-6 H-021, the only area(s)* within a building where classified information *or materials* may be handled, stored, discussed, or processed. *There are two categories of CAAs: core areas and restricted areas.*

Controlled cryptographic item (CCI): *Secure telecommunications or information system, or associated cryptographic component, unclassified and handled through the COMSEC Material Control System (CMCS), an equivalent material control system, or a combination of the two that provides accountability and visibility. Such items are marked "Controlled Cryptographic Item," or, where space is limited, "CCI".*

Controlled shipment: The transport of material from the point at which the

destination of the material is first identified for a site, through installation and/or use, under the continuous 24-hour control of Secret cleared U.S. citizens, or by DS-approved technical means and seal.

Countermeasure: *Actions, devices, procedures, or techniques that reduce a known or suspected vulnerability*.

Courier: See "Nonprofessional courier," and "Professional courier."

***Courier pouch**: See* 14 FAH-4 H-213.2*.*

CRC: An abbreviation for certification and repair center. The CRC is a facility *used by the Bureau of Information Resource Management, Deputy Chief Information Officer for Operations/Chief Technology Officer, Information Technology Infrastructure Office, Technical Security and Safeguards Division (IRM/OPS/ITI/TSS) for* program activities.

CRYPTO: A marking or designator identifying COMSEC keying material or devices used to secure or authenticate telecommunications carrying classified or sensitive national security or national security-related information.

Cryptographic access: The prerequisite to, and authorization for access to crypto information, but does not constitute authorization for use of crypto equipment and keying material issued by the Department.

Cryptographic access for use: The prerequisite to and authorization for operation, keying, and maintenance of cryptographic systems and equipment issued by the Department.

Cryptographic material: All COMSEC material bearing the marking "CRYPTO" or otherwise designated as incorporating cryptographic information.

Cryptography: The principles, means, and methods for rendering information unintelligible, and for restoring encrypted information to intelligible form.

Crypto ignition key (CIK): The device or electronic key used to unlock the secure mode of crypto equipment.

Custodian: An individual who has possession of or is otherwise charged with the responsibility for safeguarding and accounting for classified information.

Cyber infrastructure: *Includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For example: computer systems; control systems (e.g., supervisory control and data acquisition–SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure.*

***Cybersecurity* incident**: As it relates to the *Cyber Security Incident Program (CSIP),* a failure to protect the Department's cyber infrastructure from potential damage or risk.

***Cybersecurity* infraction**: *As it relates to CSIP*, one subset of a cybersecurity incident that contravenes computer security policy but does not result in damage to State's cyber infrastructure (see 12 FAM 592.1).

***Cybersecurity* violation**: *As it relates to CSIP*, the second subset of a cybersecurity incident, more serious than an infraction because it results in damage or significant risk to the Department's cyber infrastructure due to an individual's failure to comply with established Department computer security policy (see 12 FAM 592.2).

D

***Data center**: See computer room.*

Declassification: The determination that particular classified information no longer requires protection against unauthorized disclosure in the interest of national security. Such determination shall be by specific action or automatically after the lapse of a requisite period of time or the occurrence of a specified event. If such determination is by specific action, the material shall be so marked with the new designation.

Declassification event: An event that would eliminate the need for continued classification.

Decontrol: The authorized removal of an assigned administrative control designation.

***Dedicated Unclassified Space (DUS**): See* 12 FAH-6 H-542.5-13*.*

Degauss: *Procedure that reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Also called demagnetizing.*

***Denial of service**: The prevention of authorized access to resources or the delaying of time-critical operations*

Department: *Refers* to the Department of State in Washington, D.C., but not to its domestic field offices in the United States; the term "post(s)" applies to Foreign Service posts throughout the world and U.S. missions to international organizations, except those located in the United States.

Derivative classification: A determination that information is in substance the same as information currently classified, coupled with the designation of the level of classification.

***Digital signature**: An asymmetric key operation where the private key is used to digitally sign an electronic document and the public key is used to verify the signature. Digital signatures provide authenticity protection and integrity*

protection. (See electronic signature.)

Digital storage media: Flash media (e.g., universal serial bus (USB) thumb drives, digital Moving Picture Experts Group (MPEG) Audio Layer 3 (mp3) recorder/player), hard disk drives, compact disc-recordable (CD-R) disks, CD-rewritable (CD-RW) disks, digital video disc-recordable (DVD-R) disks, DVD-rewritable (DVD-RW) disks, and any other removable *or non-*removable items that can store information or data.

***Dedicated Internet Network (DIN)**: A Department owned and operated non-sensitive Unclassified local area network that supports Internet services outside the boundaries of OpenNet. A DIN can be comprised of multiple segments, where each segment is used for purposes such as: Providing public access Internet terminals; Testing of hardware and software; Local software development; Hosting services available to the Internet; To connect systems not managed by the Department (for visitors, vendors, etc.); Providing Internet access to other agencies at post; and conducting digital video conferencing over the Internet (outside the CAA).* 5 FAM 870 *provides requirements for managing DINs.*

Diplomatic courier: See "Professional courier."

Diplomatic pouch: See "U.S. diplomatic pouch."

Diplomatic Security control officer (DSCO): An individual in *Office of the Diplomatic Courier Service (DS/C/DC)* who oversees the shipment of controlled/unclassified, unpouched material from the Department to its posts worldwide. The DSCO must remain with the assigned material until it is delivered or properly secured in temporary storage. (See 12 FAM 124.)

***Disaster recovery plan**: A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.*

Disposition report: Official written correspondence relating to the determination of a charge or other legal or management action that influences the final outcome in a pending case or action.

***Distributed denial of service**: A denial of service technique that uses numerous hosts to perform the attack.*

Distributed system: *A multi-computer (e.g., workstation, terminal, server) system where more than one computer shares common system resources. The computer systems are connected to the control unit/data storage element through communication lines*.

Document: Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed material; data processing cards and tapes; maps; charts; paintings; drawings; engravings; sketches; working notes and papers; reproductions of such things by any means or process; and sound, voice, or electronic recordings in any form.

Downgrading: The determination that particular classified information requires a lesser degree of protection or no protection against unauthorized disclosure than currently provided. Such determination shall be by specific action or automatically after lapse of the requisite period of time or the occurrence of a specified event. If such determination is by specific action, the material shall be marked with the new designation.

Duration of visit or assignment: Duration of visit or assignment is described as short-term or long-term assignment. Short-term visits are one-time visits up to and including thirty (30) days or intermittent visits within a thirty-day period. Long-term visits are visits in excess of thirty days or short term intermittent visits occurring beyond a thirty-day period.

E

***Electronic signature**: The process of applying any mark in electronic form with the intent to sign a data object. See also Digital Signature.*

Encrypted text: Data encoded into an unclassified form using a nationally accepted form of encoding.

Encryption: *Conversion of plaintext to ciphertext through the use of a cryptographic algorithm.*

Endorsed Cryptographic Products List: Contains products that provide electronic cryptographic coding (encrypting) and decoding (decrypting), and have been endorsed for use on classified or Sensitive But Unclassified (SBU) U.S. Government or Government-derived information during its transmission.

***Enterprise information system/network**: See* 5 FAM 871*.*

***Enterprise mobile devices**: Devices the Department has approved to directly connect to an Enterprise network (e.g., OpenNet Blackberry, USB drive). This does not include remote access through Global OpenNet (GO).*

***Evaluation assurance level (EAL)**: A numerical grade assigned to an information technology product or system following the completion of a Common Criteria security evaluation. EAL levels are 1-7.*

***Event**: Any observable occurrence in a network or system.*

***Extension**: The extension of a Department network into non-Department space (e.g., OpenNet workstations in a contractor facility).*

F

***Federal Identity, Credential, and Access Management (FICAM)**: The Government-wide effort to provide policy and programmatic support for identity, credential, and access management business functions within the Federal Government. See FICAM Web site for more information.*

***Federal Information Security Management Act (**FISMA): A statute (Title III,*

Public Law 107-347) that requires agencies to assess risk to information systems and provide information security protections commensurate with the risk. FISMA also requires that agencies integrate information security into their capital planning and enterprise architecture processes, conduct annual information systems security reviews of all programs and systems, and report the results of those reviews to OMB.

Firecall password: *The password to a* backup user account with full administrative privileges available for use only in extenuating circumstances.

***Firewall**: A hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy.*

***Firmware**: Computer programs and data stored in hardware, typically in read-only memory (ROM) or programmable read-only memory (PROM), such that programs and data cannot be dynamically written or modified during execution of the programs.*

***Flash memory**: Electronic non-volatile memory storage device that can be electrically erased and reprogrammed.*

Foreign government information:

(1) Information provided to the United States by a foreign government or international organization of governments in the expectation, express or implied, that the information is to be kept in confidence; or

(2) Information, requiring confidentiality, produced by the United States pursuant to a written joint arrangement with a foreign government or international organization of governments. A written joint arrangement may be evidenced by an exchange of letters, a memorandum of understanding, or other written record of the joint arrangement.

Formerly restricted data: Information removed from the restricted data category upon determination jointly by the Department of Energy (DOE) and Department of Defense (DOD) that such information relates primarily to the military utilization of atomic weapons and that such information can be adequately safeguarded as classified defense information subject to the restrictions on transmission to other countries and regional defense organizations that apply to restricted data.

***Freeware**: Software available for use at no monetary cost or for an optional fee, but usually (although not necessarily) with one or more restricted usage rights (e.g., Adobe Reader, Skype).*

G

***Gateway**: A communication interface that provides compatibility between networks by converting transmission speeds, protocols, codes, or security measures.*

***General Support System (GSS)**: An interconnected set of information resources under the same direct management control which shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.*

***Guard**: Mechanism limiting the exchange of information between systems. These devices are often used between systems of different classification levels.*

H

***Hardware**: The physical parts of an information system and related devices. Internal hardware devices include motherboards, hard drives, and memory. External hardware devices include monitors, keyboards, mice, printers, scanners, tape drives, and external storage arrays.*

***High-impact system**: An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.*

***High Value Assets**: Items whose compromise or loss will severely impact post operations (personnel or payroll data, safes containing funds, Information Technology devices, etc.)*

***Hotspot**: A site that offers Internet access over a wireless local area network; no other services or data are provided*.

I

***Identification**: The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.*

Identification media: A building or visitor pass.

***Identifier**: Unique data used to represent a person or device's identity and associated attributes (e.g., username).*

***Incident response plan**: The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's information system(s).*

***Information owner**: Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.*

***Information resources**: The information and related resources, such as personnel, equipment, funds, and information technology, used by an organization.*

Information security: *The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, to provide confidentiality, integrity, and availability.*

Information system: *A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.*

Information system component: *A discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an information system.*

Information system owner: *A person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system.*

Information system security: *Protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.*

Information system security controls: *Security controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Three types of security controls:*

(1) Management: These controls focus on the management of risk and the management of information system security;

(2) Operational: These controls are primarily implemented and executed by people (as opposed to systems); and

(3) Technical: The controls are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Information system security control assessment: *The testing and/or evaluation of management, operational , and technical security controls in an information/application system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system*.

Information system security officer (ISSO): See 5 FAM 824.

Information Technology Change Control Board (IT CCB): See 5 FAM 814.

Insider: *Any person with authorized access to any United States Government resource to include personnel, facilities, information, equipment, networks or systems.*

Insider Threat: *The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.*

***Interconnection**: The linking of two distinct networks.*

***Integrity**: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity*.

Intelligence method: The method used to provide support to an intelligence source or operation, and which, if disclosed, is vulnerable to counteraction that could nullify or significantly reduce its effectiveness in supporting the foreign intelligence or foreign counterintelligence activities of the United States, or which would, if disclosed, reasonably lead to the disclosure of an intelligence source or operation.

Intelligence source: A person, organization, or technical means which provides foreign intelligence or foreign counterintelligence and which, if its identity or capability is disclosed, is vulnerable to counteraction that could nullify or significantly reduce its effectiveness in providing foreign intelligence or foreign counterintelligence to the United States. An intelligence source also means a person or organization that provides foreign intelligence or foreign counterintelligence to the United States only on the condition that its identity remains undisclosed.

***Interconnection Security Agreement (ISA)**: An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/A) between the organizations.*

***Internal system/network**: A system/network where: (i) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or (ii) cryptographic encapsulation or similar security technology provides the same effect.*

International organization: *An organization with an international membership, scope, or presence.*

Interoperable CIK: In instances where the user may require access to *more than one* vIPer , the post's designated COMSEC custodian may program the CIK devices to work in several vIPers simultaneously. These interoperable CIKS may be used to access *up to* seven STU-III terminals, depending on the model.

L

Least privilege: *Principle requiring that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use of an information system. The security objective of granting users only those accesses they need to perform their official duties.*

***Limited access area (LAA)**: See* 12 FAH-5 H-040.

Local Change Control Board (Local CCB): See 5 FAM 814.

Logged on but unattended: A workstation is considered logged on but unattended when the user is:

(1) Logged on but is not physically present in the *area*; and

(2) There is no one else present with an appropriate level of clearance safeguarding access to the workstation. Coverage must be equivalent to that which would be required to safeguard hard copy information if the same employee were away from his or her desk. Users of logged on but unattended classified workstations are subject to the issuance of security violations.

Logically disconnect: Although the physical connection between the control unit and a terminal remains intact, a system enforced disconnection prevents communication between the control unit and the terminal.

Lost pouch: Any pouch-out-of-control not recovered.

Low-Impact System: *An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.*

M

Mainframe: *A high-performance information system designed to support a large organization, handle intensive computational tasks, support a large number of users, and make use of large volumes of secondary storage.*

Major application: *An application that requires special management oversight and attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.*

Malicious code: *Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.*

Malware: *See malicious code.*

Media: *Physical devices (e.g., magnetic tapes, optical disks, magnetic disks) onto which information is stored within an information system.*

Memorandum of Understanding/Agreement (MOU/MOA): *A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission.*

Memory: *In computing, refers to the physical devices used to store programs, data, or information on a temporary or permanent basis for use in an information system or other digital electronic device.*

Message stream: The sequence of messages or parts of messages to be sent.

***Mobile code**: Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.*

***Mobile code technologies**: Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript).*

***Mobile device**: Refers to: (a) Portable removable storage media (e.g., external hard drives, USB memory sticks, flash memory cards, zip drives, IPODS, etc); and (b) portable information systems (e.g., notebook/laptop/tablet computers, personal digital assistants, BlackBerrys, smartphones, digital cameras, iPods, etc.).*

***Moderate-impact system**: An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate, and no security objective is assigned a FIPS 199 potential impact value of high.*

Modular treated conference room (MTCR): A second-generation design of the treated conference room (TCR), offering more flexibility in configuration and ease of assembly than the original TCR, designed to provide acoustic and RF emanations protection. *(Also see 12 FAH-6 H-021.)*

***Multifactor Authentication**: Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). See Authenticator.*

N

National Computer Security Center (NCSC): The NCSC is responsible for encouraging the widespread availability of trusted computer systems throughout the Federal Government.

***National Information Assurance Partnership (NIAP)**: A US government initiative to meet the security testing needs of both information technology consumers and producers operated by the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST). The long-term goal of NIAP is to help increase the level of trust consumers have in their information systems and networks through the use of cost-effective security testing, evaluation, and validation programs (e.g. Common Criteria).*

National security: The national defense or foreign relations of the United States.

National security information: Information specifically determined under executive order criteria to require protection against unauthorized disclosure.

***Near field communication (NFC)**: A set of standards for smartphones and*

similar devices to establish radio communication with each other by touching them together or bringing them into close proximity, usually no more than a few centimeters.

***Need-to-know**: A determination made by an authorized holder of information that a prospective recipient requires access to specific information to perform or assist in a lawful and authorized governmental function.*

***Network**: Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.*

***Network access**: Access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).*

Network device: An external device that can be connected to a network, including but not limited to a hub/concentrator, switch, router, printer, scanner or digital photocopier. (NOTE: Excludes internal network interfaces since internal network interfaces are considered part of an automated information system (AIS).)

***Non-Enterprise mobile devices**: Devices not approved to directly connect to an Enterprise network . This does not include remote access through Global OpenNet (GO).*

***Non-local (remote) maintenance**: Maintenance activities conducted by individuals communicating through an external network (e.g., the Internet) or an internal network from a non-Department facility (e.g., home computer).*

Nonprofessional courier: Any direct-hire, U.S. citizen employee of the U.S. Government, other than a professional diplomatic courier, who possesses a Top Secret clearance and who has been provided with official documentation (see 12 FAM 142) to transport properly prepared, addressed, and documented diplomatic pouches or controlled/unclassified material in-country, in emergencies, or when the diplomatic courier cannot provide the required service. (Clearance is preferred, but not required for handling unclassified material)

Nonrecord material: Extra and/or duplicate copies only of temporary value, including shorthand notes, used carbon paper, preliminary drafts, and other material of similar nature.

***Nonrepudiation**: Assurance the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.*

Nonsecure bulk load: A classified diplomatic pouch load in a unit load device (ULD) or other container that is not properly labeled, sealed, or built in a secure facility by appropriately cleared individuals.

***Non-volatile memory**: Memory that retains stored information even when not powered (e.g., hard drive, DVD, CD).*

O

Object: *A passive entity that contains or receives information. (See subject.)*

Object reuse: *Reassignment and re-use of a storage medium containing one or more objects after ensuring no residual data remains on the storage media*.

Off-hook: A station or trunk is off-hook when it initializes or engages in communications with the computerized telephone switch (CTS) or with another station or trunk using a link established through the CTS.

Official information: That information or material owned by, produced for or by, or under the control of the U.S. Government.

Original classification: An initial determination that information requires protection against unauthorized disclosure in the interest of national security, and a designation of the level of classification.

***Original classification authority (OCA)**: The OCA determines that unauthorized disclosure of information could reasonably be expected to result in damage to national security, and is able to identify or describe the damage in accordance with* Executive Order 13526

***Open source**: Software in which the source code is available to the general public for use and/or modification from its original design (e.g., Android operating system and is usually tied to a GNU General Public License).*

OSPB: The Overseas Security Policy Board (OSPB) is an interagency group of security professionals from the foreign affairs and intelligence communities who meet regularly to formulate security policy for U.S. missions abroad. The OSPB is chaired by the Assistant Secretary for Diplomatic Security.

***Overlay**: A specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the National Institute of Standards and Technology (NIST) 800-53 tailoring process, intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems.*

P

Pallet: *Pallets are flat platforms, usually made of metal or wood in various sizes that conform to aircraft cargo hold dimensions. Pallets can also be referred to as a ULD. (Also see Unit Load Device.)*

Palletize: The process of placing and securing classified diplomatic pouches onto a pallet in a manner that allows for handling as a single unit. *Used as a base*,

the pallets are open and exposed. Individual classified diplomatic pouches are secured *to the pallets* with nets, straps, and other restraints. This process is often referred to as palletizing or building a pallet.

Paraphrasing: A restatement of text in different phraseology without *altering* its meaning.

Password: *A protected character string used to authenticate the identity of a computer system user or to authorize access to system resources.*

PCC: An abbreviation for post communications center.

***Penetration Testing**: A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.*

Peripheral device: An external device that can be connected to a computer, including but not limited to a mouse, keyboard, printer, monitor, external Zip drive, flash drive (e.g., thumb drive), digital camera, digital voice recorder, DVD drive, DVD-RW drive, keyboard-video-mouse (KVM) switch, or scanner.

***Personal identity verification (PIV)**: The process of creating and using a Government-wide secure and reliable form of identification for Federal employees and contractors, in support of HSPD 12, Policy for a Common Identification Standard for Federal Employees and Contractors.*

***Personally Identifiable Information (PII)**: See* 5 FAM 463*.*

Plain text: Information, usually classified, in unencrypted form.

Post security officer: A U.S. citizen employee of the Foreign Service who is designated to perform security functions. At posts where regional security officers are located, they will be assigned this duty.

Pouch: See "U.S. diplomatic pouch."

Pouch Control Officer (PCO): Top Secret-cleared U.S. citizen direct-hire employee who is responsible for enforcing regulations relating to the diplomatic pouch. (*See* 14 FAM 728.1*.)*

Pouch-out-of-control: Refers to any pouch over which cleared U.S. citizen control is interrupted for any period of time making outside intervention and compromise of its contents a possibility. (See 12 FAM 130.)

Preferred Products List (PPL): A U.S. Government document that identifies information processing equipment certified by the U.S. Government as meeting TEMPEST standards. Although still valid for equipment still in use and available, the PPL has been replaced by the Evaluated Products List (EPL).

Presidential appointees: Former officials of the Department who held policy positions and were appointed by the President, by and with the advice and consent of the Senate, at the level of Ambassador, Assistant Secretary of State, or above. It does not include persons who merely received assignment commissions as Foreign Service officers, Foreign Service reserve officers,

Foreign Service staff officers, and employees.

Principal officer: Principal officer is the officer in charge of a diplomatic mission, a consular mission (other than a consular agency), or other Foreign Service post.

Product certification center: A facility which certifies the technical security integrity of communications equipment. The equipment is handled and used within secure channels.

Professional courier (or diplomatic courier): A person specifically employed and provided with official documentation (see 12 FAM 141) by the Department to transport properly prepared, addressed, and documented diplomatic pouches between the Department, its Foreign Service posts, and across other international boundaries.

***Program Manager (or Information System Owner)**: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.*

Protected distribution system (PDS): A wireline or fiber optic communications link with safeguards to permit its use for the distribution of unencrypted classified information.

Protection schema: An outline detailing the type of access users may have to a database or application system, given a user's need-to-know, e.g., read, write, modify, delete, create, execute, and append.

Public trust positions: Positions designated at either the high, moderate, or low risk level as determined by the position's potential for adverse impact to the integrity and efficiency of the service (see 5 CFR 731.106). Positions at the high or moderate risk levels are referred to as "public trust" positions and, generally, involve: policy making, major program responsibility, public safety and health, law enforcement duties, fiduciary responsibilities, or other duties/responsibilities demanding a significant degree of public trust. "Public trust" positions also involve access to, operation of, or control of proprietary systems of information (e.g., financial or personal records), with a significant risk for causing damage to people, programs or an agency, or for realizing personal gain. The "low risk" positions are, generally, referred to as "non-sensitive" positions.

R

Record material: All books, papers, maps, photographs, or other documentary materials, regardless of physical form or characteristics, made or received by the U.S. Government in connection with the transaction of public business and preserved or appropriated by an agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, or other activities of any agency of the Government, or because of the informational data contained therein.

Record traffic: Official written correspondence such as a letter, telegram, memorandum, email, or other permanent form that records, documents, or sets down in writing a way of preserving knowledge or information.

***Recovery Point Objective**: The point in time to which data must be recovered after an outage.*

***Recovery Time Objective**: The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business functions.*

Regional Diplomatic Courier Officer (RDCO): The supervising individual responsible for Diplomatic Courier operations of one of four Diplomatic Courier Service regional divisions located in Washington, D.C., Miami, Frankfurt, and Bangkok.

Regional Security Officer (RSO): Department of State, Bureau of Diplomatic Security (DS) special agents. The lead officer in a regional security office is designated the RSO and additional special agents are either deputy regional security officer (DRSO) or assistant regional security officer (ARSO). The RSO is responsible to the chief of mission at U.S. posts abroad. The RSO also receives management direction from DS through the Assistant Director for *International Programs (DS/IP).*

***Regional Computer Security Officer (RCSO**): Regional computer security officers conduct assessments of posts' cybersecurity posture to ensure technical, management, and operational controls are implemented effectively to secure information and information systems.*

Red: *In cryptographic systems, refers to information or messages that contain sensitive or classified information not encrypted. (See also Black.)*

RED/BLACK Concept: *Separation of electrical and electronic circuits, components, equipment and systems that handle unencrypted information (Red), in electrical form, from those that handle encrypted information (Black) in the same form.*

Red-Black separation: The requirement for physical spacing between "red" and "black" processing systems and their components, including signal and power lines.

Redundant control capability: Use of active or passive replacement, for example, throughout the network components (i.e., network nodes, connectivity, and control stations) to enhance reliability, reduce the threat of single point-of-failure, enhance survivability, and provide excess capacity.

***Remote access**: Refers to accessing Department SBU and/or Unclassified networks, either domestically or abroad, from Department-owned or non Department-owned systems via a Department-approved remote access program (e.g., Global OpenNet (GO), or via a Department computer located in an employee's home).*

***Remote (non-local) maintenance**: Maintenance activities conducted by individuals communicating through an external network (e.g., the Internet) or an internal network from a non-Department facility (e.g., home computer).*

Remote diagnostic facility: An off-premise diagnostic, maintenance, and programming facility authorized to perform functions on the Department computerized telephone system via an external network trunk connection.

***Remote Processing**: Refers to employees processing Department information on Department-owned or non Department-owned systems at non-Department facilities (e.g. home office).*

***Removable Media**: Portable electronic storage media such as magnetic, optical, and solid state devices, which can be inserted into and removed from a computing device and used to store text, video, audio, and image information. Examples include hard disks, zip drives, compact discs, thumb drives, pen drives, and similar USB or Thunderbolt connected storage devices.*

Restricted area: A specifically designated and posted area where classified information or material is located or where sensitive functions are performed, access controlled and only authorized personnel are admitted. *(See also 12 FAH-6 H-021.)*

Restricted data: All data (information) concerning:

(1) Design, manufacture, or use of atomic weapons;

(2) The production of special nuclear material; or

(3) The use of special nuclear material in the production of energy, but not to include data declassified or removed from the restricted data category pursuant to section 142 of the Atomic Energy Act (see section 11w, Atomic Energy Act of 1954, as amended; 42 U.S.C. 2014(y)).

RF shielding: The application of materials to surfaces of a building, room, or a room within a room, that makes the surface largely impervious to electromagnetic energy. As a technical security countermeasure, it is used to contain or dissipate emanations from information processing equipment, and to prevent interference by externally generated energy. *(See also 12 FAH-6 H-021.)*

Risk: *A measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.*

***Risk Assessment**: The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation, arising through the operation of an information system.*

RON: *Rest Remain* overnight.

S

Safeguard Officer: A cleared person who watches classified diplomatic pouches while the courier is attending to other business.

***Safeguards**: Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.*

Safekeeping: The transfer of custody of classified diplomatic pouches from a diplomatic courier for temporary storage in a secure area (such as an embassy vault). Safekeeping requires receipt of all items on a DS-7600 retained locally until custody is returned to the diplomatic courier.

***Sanitization**: Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.*

SCI: The abbreviation for sensitive compartmented information, a category of highly classified information, which requires special protection governed by the Director of the Central Intelligence Agency (CIA). *Director of National Intelligence (DNI).*

Secret-cleared U.S. citizen: A citizen of the United States who has undergone a background investigation by an authorized U.S. Government Agency and been issued a Secret security clearance, in accordance with Executive Orders 13526, and implementing guidelines and standards published in 32 CFR 147.

Secure room: Any room with floor-to-ceiling, slab-to-slab construction of some substantial material, i.e., concrete, brick, cinder block, plywood, or plaster board. Any window areas or penetrations of wall areas over 15.25 cm (*96 square* inches) must be covered with either grilling or substantial type material. Entrance doors must be constructed of solid wood, metal, etc., and be capable of holding a DS-approved three-way combination lock with interior extension. *(See also 12 FAH 5 H-456.)*

Secure voice: Systems in which transmitted conversations are encrypted to make them unintelligible to anyone except the intended recipient. Within the context of Department security standards, secure voice systems must also have protective features included in the environment of the systems terminals.

Secured domestic Department of State facility: Any building or other location in the United States or its Commonwealths or Territories staffed or managed by the Department, which the Bureau of Diplomatic Security (DS/CIS/DO) determines as warranting restricted entry.

Security anomaly: An irregularity possibly indicative of a security breach, an attempt to breach security, or of noncompliance with security standards, policy, or procedures.

***Security categorization**: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.*

Security classification designations: Refers to Top Secret, Secret, and Confidential designations on classified information or material.

Security domain: The environment of systems for which a unique security policy is applicable.

Security equipment: Protective devices such as intrusion alarms, safes, locks, and destruction equipment that provide physical or technical surveillance protection as their primary purpose.

***Security Environment Threat List**: A Department threat list intended to cover all localities operating under the authority of a chief of mission and staffed by direct-hire U.S. personnel. This list is developed in coordination with the Intelligence Community and issued annually by the Bureau of Diplomatic Security (DS).*

Sensitive *But Unclassified (SBU)* information: Information which, either alone or in the aggregate, meets any of the following criteria and is deemed sensitive by the Department, and must be protected in accordance with the magnitude of its loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data:

(1) Medical, personnel, financial, investigative, or any other information the release of which would result in substantial harm, embarrassment, inconvenience, or unfair treatment to the Department, or any individual on whom the information is maintained, such as information protected by 5 U.S.C. 522a;

(2) Information relating to the issuance or refusal of visas or permits to enter the United States, as stated in Section 222, 8 U.S.C. 1202;

(3) Information that may jeopardize the physical safety of Department facilities, personnel, and their dependents, as well as U.S. citizens abroad;

(4) Proprietary, trade secrets, commercial, or financial information the release of which would place the company or individual on whom the information is maintained at a competitive disadvantage;

(5) Information the release of which would have a negative effect on foreign policy or relations;

(6) Information relating to official travel to locations deemed to have a terrorist threat;

(7) Information considered mission-critical to an office or organization, but that is not national security information; and

(8) Information that could be manipulated to commit fraud.

Sensitive intelligence information: Such intelligence information of which unauthorized disclosure would lead to counteraction:

(1) Jeopardizing the continued productivity of intelligence sources or methods which provide intelligence vital to national security; or

(2) Offsetting the value of intelligence vital to national security.

Sensitive Personally Identifiable Information: *See* 5 FAM 463.

Sensitivity attributes: User-supplied indicators of file sensitivity the system uses to enforce an access control policy.

SEO: An abbreviation for security engineering officer.

Server room: *See computer room.*

Software: *Refers to the programs and applications that run on information systems.*

Spam: *The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.*

Special agent: A special agent in the Diplomatic Security Service (DSS) is a sworn officer of the Department or the Foreign Service, whose position is designated as either a GS-1811 or FS-2501, and has been issued special agent credentials by the Director of DSS to perform those specific law enforcement duties as defined in 22 U.S.C. 2712.

Special investigators: Contracted by the Department. Performs various non-criminal investigative functions in Diplomatic Security (DS) headquarters, field, and resident offices. They are not members of the Diplomatic Security Service (DSS) and are not authorized to conduct criminal investigations.

Spherical zone of control: A volume of space in which uncleared personnel must be escorted which extends a specific distance in all directions from TEMPEST equipment processing classified information or from a shielded enclosure. *(See also 12 FAH-6 H-021.)*

Spot Report: A timely method of keeping DS headquarters informed of fast breaking or significant events. It is a concise narrative of essential information and is afforded the most expeditious means of transmission consistent with requisite security. All courier-related Spot reports must be forwarded immediately to the DS Command Center and the Director of the Courier Service per 12 FAM 130.

Spyware: *Software secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.*

Storage object: A data object used in the system as a repository of information.

Subject: *Generally an individual, process, or device causing information to flow*

among objects or change to the system state. See Object.

***Supply Chain**: Linked set of resources and processes between multiple tiers of developers that begin with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.*

***System Access**: Ability and means to communicate with or otherwise interact with a system use system resources to handle information, gain knowledge of the information the system contains, or control system components and functions.*

System accreditation: The official authorization granted to an information system to process sensitive information in its operational environment based on a comprehensive security evaluation of the system's hardware, firmware, software security design, configuration and implementation, and other system procedural, administrative, physical, TEMPEST, personnel, and communications security controls.

System certification: The technical evaluation of a system's security features that established the extent to which a particular information system's design and implementation meets a set of specified security requirements.

System high mode: An AIS is operating in the system high mode when each user with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts has all of the following:

(1) A valid personnel clearance for all information on the AIS;

(2) Formal access approval for, and has signed nondisclosure agreements for all the information stored and/or processed; and

(3) A valid need to know for some of the information contained within the AIS.

***System owner**: Person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information or application system.*

***System security plan**: Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.*

T

Technical certification: A formal assurance by the Undersecretary for Management to Congress that standards are met that apply to an examination, installation, test, or other process involved in providing security for equipment, systems, or facilities. Certifications may include exceptions and are issued by the office or person performing the work in which the standards apply.

Technical penetration: *An unauthorized or unintentional physical or electrical connection; an unauthorized or unintentional optical, acoustic, or RF hardware*

modification, implant, software driver or firmware modification, or the unauthorized collection of fortuitous information-bearing emanations from unmodified systems, from any of these sources designed to intercept and compromise information:

(1) Known to the source;

(2) Fortuitous and unknown to the source;

(3) Clandestinely established; or

(4) Those implemented or verified through detailed physical and instrumented technical inspections, such as technical surveillance countermeasures (TSCM) operation.

Technical surveillance: The act of establishing a technical penetration and intercepting information without authorization.

Telecommunications: Any transmission, emission, or reception of signs, signals, writings, images, sounds, or information of any nature by wire, radio, visual, or other electro-magnetic, mechanical, or optical means.

***Telework**: See* 3 FAM 2361.4*.*

TEMPEST*: A short code name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information systems.*

TEMPEST equipment (or TEMPEST-approved equipment): Equipment that has been designed or modified to suppress compromising signals. Such equipment is *evaluated against National TEMPEST Standards by NSA-certified personnel and laboratories*. National TEMPEST approval does not, of itself, mean a device can be used within the foreign affairs community. Separate DS approval *in accordance with the Overseas Security Policy Board (OSPB)* is required.

TEMPEST hazard: A security anomaly that holds the potential for loss of classified information through compromising emanations.

TEMPEST test: A field or laboratory examination of the electronic signal characteristics of equipment or systems for the presence of compromising emanations.

Tenant agency: A U.S. Government Department or agency operating *abroad* as part of the U.S. foreign affairs community under the authority of a chief of mission (COM). Excluded are military elements not under direct authority of the COM.

The Vienna Convention on Diplomatic Relations (VCDR): The Vienna Convention on Diplomatic Relations is an international treaty on diplomatic intercourse and the privileges and immunities of a diplomatic mission. The VCDR sets forth law and practice on diplomatic rights and privileges.

Thin Client: Desktop workstations that rely upon an enterprise architecture, with

applications resident only on a server. The Department supports two types of thin clients:

(1) Flashless thin client, which has only random access memory (RAM) installed; and

(2) Flash thin client, which has both RAM and non-volatile FLASH memory installed. The Department configures these devices to ensure the FLASH memory acts solely to enable booting of the workstation.

Threat: *Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.*

Three-year moving window: The period of time in which the aggregate of valid (as adjudicated by DS/IS/APD) security infractions (see 12 FAM 550), or the aggregate of *cybersecurity* infractions (see 12 FAM 590) will be referred to the Bureau of Human Resources (HR) for possible disciplinary action. The period starts on the date of the last infraction and extends backward for a period of 36 months.

Top Secret-cleared U.S. citizen: A citizen of the United States who has undergone a background investigation by an authorized U.S. Government Agency and been issued a Top Secret security clearance, in accordance with *Executive Orders 13526* , and implementing guidelines and standards published in 32 CFR 147.

Treated conference room (TCR): A shielded enclosure that provides acoustic and electromagnetic attenuation protection.

Trusted computing base (TCB): The totality of protection mechanisms within an AIS (including hardware, firmware and software), the combination of which is responsible for enforcing a security policy. A trusted computing base consists of one or more components that together enforce a unified security policy over a product or AIS. The ability of a trusted computing base to correctly enforce a security policy depends solely on the mechanisms within the trusted computing base and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy.

***Trusted Internet Connections (TIC) Initiative**: The TIC Initiative, as outlined in OMB Memorandum M-08-05 (PDF, 1 page - 28 KB), is to optimize and standardize the security of individual external network connections currently in use by Federal agencies, including connections to the Internet.*

***Two factor authentication**: The use of two types of authentication factors from the following: (1) something the user KNOWS (e.g., password), and (2) something the user HAS (e.g., the one-time FOB); (3) or something the user IS (e.g., fingerprint).*

Type I: Type I products are designed to secure classified information but may also be used to protect sensitive unclassified information.

U

Unauthorized disclosure: The compromise of classified information by communication or physical transfer to an unauthorized recipient. It includes the unauthorized disclosure of classified information in a newspaper, journal, or other publication where such information is traceable to an agency because of a direct quotation, or other uniquely identifiable fact.

***Unclassified controlled air pouch (UCAP)**: See* 14 FAH-4 H-213.1-5*.*

Unit load device (ULD): Aviation terminology referring to a pallet or container used to load freight (i.e., *U.S.* diplomatic pouches) on wide-body aircraft and specific narrow-body aircraft. It allows a large quantity of cargo to be bundled into a single unit that can be lifted by mechanical devices.

Unit security officer: A U.S. citizen employee who is a nonprofessional security officer designated with a specific or homogeneous working unit to assist the office of security in carrying out functions prescribed in these regulations.

United States and its Territories: The 50 States; the District of Columbia; the Commonwealth of Puerto Rico; the Territories of Guam, American Samoa, the U.S. Virgin Islands; and the Possessions—Midway and Wake Islands.

Upgrading: The determination that particular unclassified or classified information requires a higher degree of protection against unauthorized disclosure than currently provided. Such determination shall be coupled with a marking of the material with the new designation.

U.S. diplomatic pouch: A properly documented, sealed bag, briefcase, envelope, or other container. It is used to transmit approved correspondence, documents, publications, and other *items* for official use between the Department *of State, U.S. Diplomatic posts*, and between *U.S. Diplomatic* posts. (See 14 FAH-4 H-213.1-5

***User**: Individual, or (system) process acting on behalf of an individual, authorized to access an information system.*

***User ID**: Unique character string used by an information system to identify a specific user.*

V

Vienna Convention: The Vienna Convention on Diplomatic Relations (see 12 FAM 111.2), which sets forth law and practice on diplomatic rights and privileges. Couriers must follow these guidelines to ensure that diplomatic rights and privileges are not infringed upon. (See 12 FAM 123.)

Visa fraud: The fraudulent procuring, forging, or fraudulent use of visas or other

entry documents.

Visitor: Any person not issued a permanent building pass, who seeks to enter any Department facility for work, consultation, or other legitimate reason.

Visitor passes: Passes of limited duration that DS issues to visitors at designated Department facilities. These also include conference or other special function passes.

Volatile memory: *Memory that requires power to maintain the stored information. Volatile memory retains the information as long as there is a power supply, but when there is no power supply, the stored information is lost.*

Vulnerability: *Weakness in a facility, equipment, information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.*

W

Weingarten Rights: Rights afforded to an employee who is a member of a collective bargaining unit for which a union representative has exclusive representation rights. When the employee is to be personally interviewed and reasonably believes the interview may result in disciplinary action against him or her, the investigating official must give the employee the opportunity to be represented by the exclusive representative, if the employee so requests.

Whitelisting: *The process used to identify: (i) software programs authorized to execute on an information system; or (ii) authorized Universal Resource Locators (URL)/Web sites.*

Wireless technology: *Technology that permits the transfer of information between separated points without physical connection.*

Workbag: A larger diplomatic pouch used to consolidate smaller classified diplomatic pouches. It is usually secured with a pouch seal or the courier's personal lock. Only other diplomatic pouches, official correspondence, or documents intended exclusively for official use may be transported inside the workbag. Personal items are not allowed.

12 FAM 092 THROUGH 099 UNASSIGNED