# 12 FAM 090
# DEFINITIONS OF DIPLOMATIC SECURITY TERMS

*(TL:DS-95; 11-14-2003)*
*(Office of Origin: DS/PPB/PPD)*

## 12 FAM 091 TERMS

*(TL:DS-95; 11-14-2003)*

### A

**Access**: The ability and the means necessary to read, store, or retrieve data, to communicate with, or to make use of any resource of an automated information system.

**Access control**: The process of limiting access to the resources of a system only to authorized programs, processes, or other systems (in a network). Synonymous with controlled access and limited access.

**ACR**: Abbreviation for acoustic conference room, an enclosure which provides acoustic but not electromagnetic emanations shielding; ACRs are no longer procured; TCRs are systematically replacing them.

**Advisory sensitivity attributes**: User-supplied indicators of file sensitivity that alert other users to the sensitivity of a file so that they may handle it appropriate to its defined sensitivity. Advisory sensitivity attributes are not used by the AIS to enforce file access controls in an automated manner.

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

**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. Noncontrolled access areas are spaces where classified operations/discussions/storage do not occur.

**ASE**: Abbreviation for acoustical shielded enclosure.

**Audit log/trail**: Application or system programs when activated automatically monitor system activity in terms of on-line users, accessed programs, periods of operation, file accesses, etc.

**Authenticate**:

(1) To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system; and

(2) To verify the integrity of data that otherwise have been stored, transmitted, or exposed to possible unauthorized modification.

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

**Automated information system (AIS)**:

(1) An assembly of computer hardware, software, firmware, and related peripherals configured to collect, create, compute, disseminate, process, store, and/or control data or information; and

(2) Information systems that manipulate, store, transmit, or receive information, and associated peripherals such as input/output and data storage and retrieval devices and media.

# B

**Black**: In the information processing context, black denotes data, text, equipment, processes, systems or installations associated with unencrypted information that requires no emanations security related protection. For example, electronic signals are “black” if bearing unclassified information. Antonym: Red.

**Building passes**: Those passes the Bureau of Diplomatic Security (DS) issues to permanent Department of State 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 DOS 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.

# C

**C2**: A formal product rating awarded to a product by the National Computer Security Center (NCSC). A C2-rated system incorporates controls capable of enforcing access limitations on an individual basis, making users individually accountable for their actions through logon procedures, auditing of security relevant events, and resource isolation.

**"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 that are performed by groups other than those who normally accomplish these tasks.

**Central Office of Record (COR)**: The Department element which 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, Secret, or Confidential.

**Classification authority**: The authority vested in an official of an agency to originally classify information or material which is determined by that official to require protection against unauthorized disclosure in the interest of national security.

**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 information**: Information or material, herein collectively termed information, that is owned by, produced for or by, or under the control of the U.S. Government, and that has been determined pursuant to Executive Order 12958 or prior orders to require protection against unauthorized disclosure, coupled with the designation of the 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 Part 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**: National security information classified in accordance with E.O. 12356, dated April 2, 1982.

**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 (i.e., CIHS, C-Lan) of, principally, access rights and information distribution;

(3) A telecommunications processor (i.e., TERP, IMH) 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.

**Composite Threat List**: A Department of State 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 semiannually by the Bureau of Diplomatic Security.

**Compromise**: Loss of security enabling unauthorized access to classified information. Affected material is not automatically declassified.

**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, typewriters) which process national security information.

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

**COMSEC custodian**: The properly-appointed individual who manages, controls, and is accountable for COMSEC material charged to the facility account. Only Department of State personnel will be appointed.

**COMSEC facility**: Space employed for the purpose of generating, storing, repairing, or using COMSEC material.

**COMSEC material**: The term which nominally covers any means or method used to apply COMSEC security. It includes, but is not limited to:

(1) Key;

(2) Equipment;

(3) Devices;

(4) Firmware;

(5) Software;

(6) Controlled cryptographic items (CCI);

(7) Information (manuals, CRYPTO-logic);

(8) Material marked CRYPTO; and

(9) Any other items developed or produced to perform COMSEC functions.

**COMSEC Material Control System (CMCS)**: The logistics and accounting system through which COMSEC material is distributed, controlled, and safeguarded.

**COMSEC officer**: The properly appointed individual responsible to ensure that COMSEC regulations and procedures are understood and adhered to, that the COMSEC facility is operated securely, that personnel are trained in proper COMSEC practices, and who advises on communications security matters. Only Department of State personnel will be appointed.

***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 Orders 12968 and 10450 and implementing guidelines and standards published in 32 CFR Part 147.*

**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 pub-

lic 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 AC- or battery-powered, which are not part of the facility infrastructure. Some examples are radios, televisions, electronic recording or playback equipment, PA systems, paging devices, and dictaphones (see also electronic equipment).

**Controlled access area**: Controlled access areas are specifically designated areas within a building where classified information may be handled, stored, discussed, or processed.

**Controlled cryptographic item (CCI)**: Secure telecommunications or information handling equipment, or associated cryptographic components, which are unclassified but governed by a special set of control requirements.

**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.

**Courier**: See “Nonprofessional courier,” and “Professional courier.”

**CRC**: An abbreviation for certification and repair center. The CRC is a facility utilized by IM/SO/TO/OTSS 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.

# D

**D2**: A rating provided by the NCSC for PC security subsystems which corresponds to the features of the C2 level. A computer security subsystem is any hardware, firmware and/or software which are added to a computer system to enhance the security of the overall system.

**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 which would eliminate the need for continued classification.

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

**Degauss**: To apply a variable, alternating current (AC) field for the purpose of demagnetizing magnetic recording media. The process involves increasing the AC field gradually from zero to some maximum value and back to zero, which leaves a very low residue of magnetic induction on the media.

**Department**: Applies 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.

**Diplomatic courier**: See “Professional courier.”

**Diplomatic pouch**: See “U.S. diplomatic pouch.”

**Diplomatic Security control officer (DSCO)**: An individual in DS/CIS/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.)

**Distributed system**: A multi-work station, or terminal system where more than one workstation shares common system resources. The work stations 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.

**DOSTN**: An abbreviation for "Department of State Telecommunications Network." DOSTN is a "black" transmission facility.

**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 so 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

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

**Encryption**: The translation of plain text into an unintelligible form in order to render the information meaningless to anyone who does not possess the decoding mechanism.

**Endorsed Cryptographic Products List**: Contains products that provide electronic cryptographic coding (encrypting) and decoding (decrypting), and which have been endorsed for use in classified or sensitive unclassified U.S. Government or government-derived information during its transmission.

**Endorsed TEMPEST Products List**: A list of commercially developed and commercially produced TEMPEST telecommunications equipment that NSA has endorsed, under the auspices of the NSA Endorsed TEMPEST Products Program, for use by government entities and their contractors to

process classified U.S. Government information.

**Escort**: A cleared U.S. citizen at post who assists couriers with arrivals and departures. (See 12 FAM 152.1.)

# F

**Firecall password**: A backup user account with full administrative privileges that is available for use only in extenuating circumstances.

**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 and Department of Defense 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.

# I

**Identification media**: A building or visitor pass.

**Information security**: Safeguarding information against unauthorized disclosure; or, the result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information the protection of which is authorized by Executive Order or statute.

**Information systems**: A combination of AIS and communications equipment, software, and related devices.

**Intelligence method**: The method which is 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 which provides foreign intelligence or foreign counterintelligence to the United States only on the condition that its identity remains undisclosed.

**International organization**: An organization of governments.

**Interoperable CIK**: In instances where the user may require access to other STU-III terminals, the post's designated COMSEC custodian may program the CIK devices to work in several STU-III terminals simultaneously. These interoperable CIKS, if desired, may be used to access as many as seven other 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.

**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 office; 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 which is not recovered.

# M

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

**Modular treated conference room (MTCR)**: A second-generation design of the treated conference room (TCR), offering more flexibility in con-

figuration and ease of assembly than the original TCR, designed to provide acoustic and RF emanations protection.

# N

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

**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.

**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 that are only of temporary value, including shorthand notes, used carbon paper, preliminary drafts, and other material of similar nature.

# O

**Object**: From the Orange Book definition, "A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are: records, blocks, pages, files, directories and programs, as well as bits, bytes, words, fields, keyboards, clocks, printers, network nodes, etc."

**Object reuse**: The reassignment to a subject (e.g., a user) of a medium that previously contained an object (e.g., a file). The danger of object reuse is that the object may still contain information that the subject may not be authorized to access. Examples are magnetic tapes that haven't been erased or workstations that hold information in local storage.

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

**Official information**: That information or material which is owned by,

produced for or by, or under the control of the U.S. Government.

**OISS controlled item**: OISS or other equipment placed under the control process used for OISS.

**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 classifier**: An authorized individual in the executive branch who initially determines that particular information requires a specific degree of protection against unauthorized disclosure in the interest of national security and applies the classification designation “Top Secret,” “Secret,” or “Confidential.”

**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 Director, Diplomatic Security Service.

# P

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

**Password**: A protected string of characters that authenticates a user, specific resource, or access type.

**PCC**: An abbreviation for post communications center.

**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-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 which is 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 of State who held policy positions and were appointed by the President, by and with the advise 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.

**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 U.S. Department of State to transport properly prepared, addressed, and documented diplomatic pouches between the Department and its Foreign Service posts and across other international boundaries.

**Protected distribution system (PDS)**: A wireline or fiberoptic 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.

# R

**RDCO**: Regional diplomatic courier officer. The RDCO oversees the operations of a regional diplomatic courier division.

**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.

**Red**: In the information processing context, it denotes encrypted/classified data, text, equipment, processes, systems or installations associated with information that requires emanations security protection. For example, wiring that carries unencrypted classified information either exclusively or mixed with unclassified is termed "red" wiring. Antonym: Black.

**RED/BLACK Concept**: The separation of electrical and electronic circuits, components, equipment, and systems which handle classified plain text (RED) information in electrical signal form from those which handle unclassified (BLACK) information 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 threat of single point-of-failure, enhance survivability, and provide excess capacity.

**Regional security officer**: A professionally trained officer who has been designated to administer the security program for a specific area or post.

**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.

**Restricted area**: A specifically designated and posted area in which classified information or material is located or in which sensitive functions are performed, access to which is controlled and to which only authorized personnel are admitted.

**Restricted data**: All data (information) concerning:

(1) Design, manufacture, or utilization 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.

**Risk**: A measurement of the likelihood of compromise of information, and the damage to U.S. interests that would result. Risk is determined by threat, vulnerability, and sensitivity of the information stored or processed at post.

# S

**Sanitize**: The degaussing or overwriting of information on magnetic or other storage media.

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

***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 12968 and 10450 and implementing guidelines and standards published in 32 CFR Part 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 (six 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.

**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 of State 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 classification designations**: Refers to “Top Secret,” and “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 which provide physical or technical surveillance protection as their primary purpose.

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

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

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

**Sensitive unclassified information**: Information which, either alone or in the aggregate, meets any of the following criteria and is deemed sensitive by the Department of State, 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 which 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 which is not national security information; and

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

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

**SEO**: An abbreviation for security engineering officer.

**Special agent**: A special agent in the Diplomatic Security Service is a sworn officer of the Department of State 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 the Diplomatic Security Service to perform those specific law enforcement duties as defined in 22 U.S.C. 2712.

**Special investigators**: Special investigators are contracted by the Department of State. They perform various non-criminal investigative func-

tions in DS headquarters, field, and resident offices. They are not members of the Diplomatic Security Service 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.

**Storage media**: Floppy diskettes, tapes, hard disk drives, or any devices that store automated information.

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

**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, and software security design, configuration and implementation and of the 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.

# T

**Technical certification**: A formal assurance by the Undersecretary for Management to Congress that standards are met which 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 RF, acoustic, or emanations

intercept of information. This intercept may occur along a transmission path which is:

(1) Known to the source;

(2) Fortuitous and unknown to the source; or

(3) Clandestinely established.

**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.

**TEMPEST**: The name given to investigations and studies of compromising emanations.

**TEMPEST-approved personal computer (TPC)**: A personal computer that is currently listed on the Preferred Products List (PPL) or Evaluated Products List (EPL).

**TEMPEST-certification**: Nationally approved hardware that protects against the transmission of compromising emanations, i.e., unintentional signals from information processing equipment which can disclose information being processed by the system.

**TEMPEST equipment (or TEMPEST-approved equipment)**: Equipment that has been designed or modified to suppress compromising signals. Such equipment is approved at the national level for U.S. classified applications after undergoing specific tests. National TEMPEST approval does not, of itself, mean a device can be used within the foreign affairs community. Separate DS approval 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 overseas as part of the U.S. foreign affairs community under the authority of a chief of mission. Excluded are military elements not under direct authority of the chief of mission.

**Threat**: In the security technology context, the likelihood that attempts will be made to gain unauthorized access to information or facilities.

***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 12968 and 10450 and implementing guidelines and standards published in 32 CFR Part 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.

**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.

**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, and the U.S. Virgin Islands; the Trust Territory of the Pacific Islands; the Canal Zone; 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 articles for official use between the Department and post and between posts. (See 5 FAM.)

**User's identification**: A character string which validates authorized user access.

## 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 section 12 FAM 123 and 12 FAM 111 Exhibit 111.2.)

**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 of State (DOS) facility for work, consultation, or other legitimate reason.

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

**Vulnerability**: The susceptibility of a facility, system or equipment to penetration by technical means.

# 12 FAM 092 THROUGH 099 UNASSIGNED