



October 2011

Glossary

of SECURITY TERMS, DEFINITIONS,
and ACRONYMS

Center for Development of Security Excellence

CDSE

Learn. Perform. Protect.

Glossary Terms 04

A	05
B	19
C	22
D	53
E	71
F	80
G	93
H	96
I	99
J	114
K	115
L	116
M	121
N	127
O	134
P	142
Q	160
R	161
S	170
T	196
U	208
V	214
W	216

Note: To return to the TOC, click the button at the bottom left of each glossary page

Acronym Terms	217
A	219
B	223
C	224
D	232
E	237
F	238
G	241
H	242
I	243
J	247
K	248
L	248
M	250
N	252
O	258
P	260
Q	264
R	264
S	266
T	272
U	275
V	277
W	277
X	278
Y	278

Note: To return to the TOC, click the button at the bottom left of each acronym page

Glossary Terms

Acceptable Level of Risk

Authority determination of the level of potential harm to an operation, program, or activity as a result of a loss of information that the authority is willing to accept.

Access

The ability and opportunity to obtain knowledge of classified information.

Accesses

Indoctrination to classified material that has additional security requirements or caveats. This may be Sensitive Compartmented Information, Special Access Program information, or collateral level accesses such as North Atlantic Treaty Organization, Critical Nuclear Weapons Design Information, etc.

Access Approval

Formal authorization for an individual to have access to classified or sensitive information within a Special Access Program or a Controlled Access Program, including Sensitive Compartmented Information. Access requires formal indoctrination and execution of a non-disclosure agreement.

Access Approval Authority

Individual responsible for final access approval and/or denial determination.

Access Control

The process of granting or denying specific requests:

- (1) for obtaining and using information and

related information processing services
(2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).

Access Control Mechanisms

Measures or procedures designed to prevent unauthorized access to protected information or facilities.

Access Eligibility Determination

A formal determination that a person meets the personnel security requirements for access to a specified type or types of classified information.

Access Evaluation

The process of reviewing the security qualifications of employees.

Accessioned Records

Records of permanent historical value in the legal custody of National Archives and Records Administration.

Access National Agency Check with Inquiries

A personnel security investigation for access to classified information conducted by the Office of Personnel Management, combining a national agency check and written inquiries to law enforcement agencies, former employers and supervisors, references, and schools, and a credit check; this is only conducted on Civilian employees and does not apply to Military or Contractor personnel

Access Roster

A database or listing of individuals briefed to a Special Access Program.

Access Termination

The removal of an individual from access to Special Access Program or other program information.

Accountability

Assigning of a document control number (including copy #) which is used to establish individual responsibility for the document and permits traceability and disposition of the document.

Accreditation

Formal declaration by the DAA that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

Accredited Security Parameter

The security classification levels, compartments and sub-compartments at which an Information System or network is accredited to operate [e.g. Top Secret or Special Access Required]

Accreditation (of Information System)

The approval to use an Information System to process classified information in a specified environment at an acceptable level of risk based upon technical, managerial and procedural safeguards.

Accrediting Authority

Synonymous with Designated Accrediting Authority (DAA). See also Authorizing Official.

Acknowledged Special Access Program

A Special Access Program that is acknowledged to exist and whose purpose is identified (e.g., the B-2 or the F-117 aircraft program) while the details, technologies, materials, techniques, etc., of the program are classified as dictated by their vulnerability to exploitation and the risk of compromise. Program funding is generally unclassified. (Note: Members of the four Congressional Defense Committees are authorized access to the program)

Acoustical Intelligence

Intelligence information derived from the collection and analysis of acoustical phenomena.

Acoustical Security

Those security measures designed and used to deny aural access to classified information.

Acquisition Program

An Acquisition Program is a directed, funded effort that provides a new, improved, or continuing materiel, weapon or information system, or service capability in response to an approved need.

Acquisition Special Access Program

A special access program established primarily to protect sensitive research, development, testing, and evaluation or procurement activities in support of sensitive military and intelligence requirements.

Acquisition Systems Protection

The safeguarding of defense systems anywhere in the acquisition process as defined in Department of Defense Directive 5000.1, the defense technologies being developed that could lead to weapon or defense systems, and defense research data. Acquisition Systems Protection integrates all security disciplines, counterintelligence, and other defensive methods to deny foreign collection efforts and prevent unauthorized disclosure, to deliver to our forces uncompromised combat effectiveness over the life expectancy of the system.

Activity

A Department of Defense unit, organization, or installation performing a function or mission.

Activity Security Manager

The individual specifically designated in writing and responsible for the activity's information security program which ensures that classified and controlled unclassified information is properly handled during its entire life cycle. This includes ensuring it is appropriately identified, marked, stored, disseminated, disposed of, and accounted for, as well as providing guidance on the handling of security incidents to minimize adverse effects and ensure that appropriate corrective action is taken. The security manager may be assigned responsibilities in other security disciplines such as personnel and physical security, etc.

Adjudication

Evaluation of personnel security investigations and other relevant information to determine if it is clearly consistent with the interests of national security for persons to be granted (or retain) eligibility for access to classified information, and/or continue to hold positions requiring a trustworthiness decision.

Adjudication Authority

Entity which provides adjudication for eligibility or access.

Adjudicative Process

An examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk.

Adjudicator

A personnel security specialist who performs adjudications.

Adversary

An individual, group, organization or government that must be denied Critical Program Information. Synonymous with competitor/enemy.

Adversary Collection Methodology

Any resource and method available to and used by an adversary for the collection and exploitation of sensitive/critical information or indicators thereof.

Adversary Threat Strategy

The process of defining, in narrative or graphical format, the threat presented to an operation,

program, or project. The adversary threat strategy should define the potential adversaries, the courses of action those adversaries might take against the operation, and the information needed by the adversaries to execute those actions.

Adverse Action

A removal from employment, suspension from employment of more than 14 days, reduction in grade, reduction of pay or furlough of 30 days or less.

Adverse Information

Any information that adversely reflects on the integrity or character of a cleared employee that suggests that his or her ability to safeguard classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of national security.

Affiliate

Any entity effectively owned or controlled by another entity.

Agency

Any "Executive agency," as defined in 5 U.S.C. 105, and any other entity within the executive branch that comes into the possession of classified information.

Agent

A person who engages in a clandestine activity.

Agent of the Government

A contractor employee designated in writing

by the Government Contracting Officer who is authorized to act on behalf of the Government.

Alien

Any person who is not a citizen of the United States.

Alternative Compensatory Control Measures

Used to safeguard sensitive intelligence or operations and support information (acquisition programs do not qualify) when normal measures are insufficient to achieve strict need-to-know controls, and where Special Access Program controls are not required.

Analysis

The process by which information is examined in order to identify significant facts and/or derive conclusions.

Anti-Tamper

Systems engineering activities intended to deter and/or delay exploitation of critical technologies in a U.S. defense system in order to impede countermeasure development, unintended technology transfer, or alteration of a system.

Anti-Tamper Executive Agent

The Department of Defense Anti-Tamper Executive Agent, chartered by the Under Secretary of Defense (Acquisition, Technology, and Logistics), and assigned to the Directorate for Special Programs, Office of the Assistant Secretary of the Air Force for Acquisition.

Appeal

A formal request under the provisions of Executive Order 12968, Section 5.2, for review of a denial or revocation of access eligibility.

Applicant

A person other than an employee who has received an authorized conditional offer of employment for a position that requires access to classified information.

Application

Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring or administrative privileges. Examples include office automation, electronic mail, web services, and major functional or mission software programs.

Approved Access Control Device

An access control device that meets the requirements of the NISPOM as approved by the Facility Security Officer.

Approved Built-in Combination Lock

A combination lock, equipped with a top-reading dial that conforms to Underwriters Laboratory Standard Number UL 768 Group IR.

Approved Combination Padlock

A three-position dial-type changeable combination padlock listed on the Government Services Administration Qualified Products List as meeting the requirements of Federal Specification FF-P-110.

Approved Electronic, Mechanical, or Electro-Mechanical Device

An electronic, mechanical, or electro-mechanical device that meets the requirements of Department of Defense 5220.22-M as approved by the Facility Security Officer.

Approved Key-Operated Padlock

A padlock, which meets the requirements of MIL-SPEC-P-43607 (shrouded shackle), National Stock Number 5340-00-799-8248, or MIL-SPEC-P-43951 (regular shackle), National Stock Number 5340-00-799-8016.

Approved Security Container

A security file container, originally procured from a Federal Supply Schedule supplier that conforms to federal specifications and bears a "Test Certification Label" on the locking drawer attesting to the security capabilities of the container and lock. Such containers will be labeled "General Services Administration Approved Security Container" on the face of the top drawer. Acceptable tests of these containers can be performed only by a testing facility specifically approved by General Services Administration.

Approved Vault

A vault constructed in accordance with Department of Defense 5220.22-M and approved by the Cognizant Security Agency.

Approved Vault Door

A vault door and frame unit originally procured from the Federal Supply Schedule (Federal Supply Classification Group 71, Part III, Section E, Federal Supply Classification Class 7110), that meets Federal Specification AA-D-600.

Assessment

To evaluate the worth, significance, or status of something; especially to give an expert judgment of the value or merit of something.

Asset

A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

Associated (Enhanced) Markings

Markings, other than those which designate classification level, that are required to be placed on classified documents. These include the “classified by” line, downgrading and declassification instructions, special control notices, Special Access Program caveats, etc.

Astragal Strip A narrow strip of material applied over the gap between a pair of doors for protection from unauthorized entry and sound attenuation.

Authentication

The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data. Verifying the identity of a

user, process, or device, often as a prerequisite to allowing access to resources in an IS.

Authenticity

Having an undisputed identity or origin.

Authorized Adjudicative Agency

An agency authorized by law or regulation, or direction of the Director of National Intelligence to determine eligibility for access to classified information in accordance with Executive Order 12698.

Authorized Classification and Control Markings Register

Also known as the “CAPCO Register”, this is the official list of authorized security control markings and abbreviated forms of such markings for use by all elements of the Intelligence Community for classified and unclassified information.

Authorized Person

A person who has a need-to-know for classified information in the performance of official duties and who has been granted a Personnel Security Clearance (PCL) at the required level.

Authorized Investigative Agency

Any agency authorized by law, executive order, regulation or Director, Office of Management and Budget under Executive Order 13381 to conduct counterintelligence investigations or investigations of persons who are proposed for access to sensitive or classified information to ascertain whether such persons satisfy the criteria

for obtaining and retaining access to such information.

Authorized User

Any appropriately cleared individual with a requirement to access a Department of Defense information system in order to perform or assist in a lawful and authorized governmental function.

Automated Information System

A generic term applied to all electronic computing systems. Automated Information System's are composed of computer hardware (i.e., automated data processing equipment and associated devices that may include communication equipment), firmware, operating systems, and other applicable software.

Automated Information System's collect, store, process, create, disseminate, communicate, or control data or information.

Automated Information System Media Control System

A system of procedures, approved by the Program Security Officer, which provide controls over use, possession, and movement of magnetic media in Special Access Program Facility. The procedures must insure all magnetic media (classified and unclassified) are adequately protected to avert the unauthorized use, duplication, or removal of the media. The media must be secured in limited access containers or labeled with the Identity of the individual responsible for maintaining the material.

Automatic Declassification

The declassification of information based solely upon the occurrence of a specific date or event as determined by the original classification authority, or the expiration of a maximum time frame for duration of classification established under this order.

Availability

The property of being accessible and useable upon demand by an authorized entity. Ensuring timely and reliable access to and use of information. destruction of materials deemed Classified.

Background Investigation

A personnel security investigation consisting of both record reviews and interviews with sources of information covering the most recent 5 years of an individual's life or since the 18th birthday, whichever is shorter, provided that at least 2 years are covered and that no investigation will be conducted prior to an individual's 16th birthday.

Balanced Magnetic Switch

A type of intrusion detection system sensor which may be installed on any rigid, operable opening (i.e., doors, windows) through which access may be gained to the Special Access Program Facility and Sensitive Compartmented Information.

Beta I

Security Certification testing performed in a lab environment or other facility as appropriate.

Beta II

Security Certification testing performed at designated operational installations (s) until stable baseline is achieved (configuration differences or other factors may necessitate multiple Beta II test sites).

Billets

A determination that in order to meet need-to-know criteria, certain Special Access Programs may elect to limit access to a predetermined number of properly cleared employees. Security personnel do not count against the billet system.

BLACK

A designation applied to wire lines, components, equipment,

Boundary

Physical or logical perimeter of a system.

Break-Wire Detector

An Intrusion Detection System sensor used with screens and grids, open wiring, and grooved stripping in various arrays and configurations necessary to detect surreptitious and forcible penetrations of movable openings, floors, walls, ceilings, and skylights. An alarm is activated when the wire is broken.

Burn Bag

The informal name given to a container (usually a paper bag or some other waste receptacle) that holds sensitive or classified documents which are to be destroyed by fire or pulping after a certain period of time. The most common usage of burn bags is by government institutions, in the destruction of materials deemed Classified.

Burn-In

A tendency for an image that is shown on a display over a long period of time to become permanently fixed on the display. This is most often seen in emissive displays such as Cathode Ray Tube and Plasma because chemical change can occur in the phosphors when exposed repeatedly to the same electrical signals.

BUSTER

A computer program-part of the Computer Security Tool-box. BUSTER is a MS-DOS based program used to perform a binary search of a disk or diskette for any word or set of words found in a search definition file by performing a linear search on a disk or diskette, four sectors at a time.

Camouflage

The use of natural or artificial material on personnel, objects, or positions (e.g., tactical) in order to confuse, mislead, or evade the enemy/adversary.

Carve-Out

A classified contract for which the Defense [Security] Service has been relieved of inspection responsibility in whole or in part

Case Officer

A professional employee of an intelligence organization who is responsible for providing direction for an agent operation. See the individual components: camouflage; concealment; and deception.

Case-by-Case Basis

The principle that a disclosure authorization is restricted to individual events or occasions to prevent confusion with permanent and repetitive disclosure determinations.

Caveat

A designator used with or without a security classification to further limit the dissemination of restricted information, e.g., For Official Use Only and Not Releasable to Foreign Nationals

Central Adjudication Facility

A single facility designated by the head of the Department of Defense Component to evaluate personnel security investigations and other relevant information.

Central United States Registry for North Atlantic Treaty Organization

North Atlantic Treaty Organization controls its classified records through a registry system, in which individual documents are numbered and listed in inventories. The Central United States Registry is located in Arlington, Virginia, and oversees more than 125 sub-registries in the U.S. and abroad.

Certification

Comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meets a set of specified security requirements.

Certified TEMPEST Technical Authority

A United States Government employee who has met established certification requirements in accordance with the Committee on the National Security Systems approved criteria and has been appointed by a United States Government department or agency to fulfill Certified TEMPEST Technical Authority responsibilities.

Classification

The act or process by which information is determined to be classified information, classified National Security information (or "Classified Information"). Information that has been determined pursuant to Executive Order 13526, as amended or any predecessor order to require protection against unauthorized disclosure and is

marked to indicate its classified status when in documentary form.

Classification Guidance

Any instruction or source that prescribes the classification of specific information.

Classification Guide

A documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

Classification Levels

Information may be classified at one of the following three levels: TOP SECRET, which is applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe: SECRET, which is applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe: and CONFIDENTIAL, which is applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

Classification Markings and Implementation Working Group

An Intelligence Community forum of Intelligence Community and non-Intelligence Community members that is responsible for coordinating changes to the Authorized Classification and Control Markings Register and associated implementation manual.

Classified Contract

Any contract requiring access to classified information by a contractor or his or her employees in the performance of the contract. (A contract may be referred to as a “classified contract” even though the contract document is not classified.) The requirements prescribed for a “classified contract” (in the NISPOM and other relevant issuances) also are applicable to all phases of precontract activity, including solicitations (bids, quotations, and proposals), precontract negotiations, post-contract activity, or other Government Contracting Agency (GCA) program or project which requires access to classified information by a contractor.

Classified National Security Information

Official information or material that requires protection in the interests of national security and that is classified for such purpose by appropriate classifying authority in accordance with the provisions of Executive Order 13526. Also known as “Classified Information”.

Classified Information Procedures Act

A law that provides a mechanism for the courts to determine what classified information defense counsel may access.

Classified Military Information

Information originated by or for the Department of Defense or its Agencies or is under their jurisdiction or control and that requires protection in the interests of national security. It is designated TOP SECRET, SECRET, or CONFIDENTIAL. Classified Military Information may be conveyed via oral, visual, or material form.

Classified Visit

A visit during which a visitor will require, or is expected to require, access to classified information.

Classifier

Any person who makes a classification determination and applies a classification category to information or material. The determination may be an original classification action or it may be a derivative classification action. Contractors make derivative classification determinations based on classified source material, a security classification guide, or a Contract Security Classification Specification.

Clearance

Formal certification of authorization for a person or contractor to have access to classified information, other SCI, or information protected in a SAP. Clearances are of three types:

Confidential, secret, and Top Secret. A Top Secret clearance permits access to Top Secret, Secret, and Confidential material; a Secret clearance, to Secret and Confidential material; and a Confidential clearance, to Confidential material.

Clearance Certification

An official notification that an individual holds a specific level of security clearance and/or access approval(s), authorizing the recipient of the certification access to classified information or materials at that level.

Cleared Commercial Carrier

A carrier that is authorized by law, regulatory body, or regulation, to transport SECRET and CONFIDENTIAL material and has been granted a SECRET facility clearance in accordance with the National Industrial Security Program.

Cleared Employees

All contractor employees granted Personnel Security Clearances and all employees being processed for Personnel Security Clearances.

Related to Clearance; Security Clearance.

Cleared Escort An appropriately cleared United States citizen, at least 18 years old, who performs access control/escort duties on limited and minor construction, repair or maintenance projects in Sensitive Compartmented Information Facilities or other classified areas that do not require a Construction Surveillance Technician.

Clearing

Removal of data from an IS, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capabilities (i.e., through the keyboard); however, the data may be reconstructed using laboratory methods.

Closed Area

An area that meets the requirements of the NISPOM for safeguarding classified material that, because of its size, nature, or operational necessity, cannot be adequately protected by the normal safeguards or stored during nonworking hours in approved containers.

Closed Storage

The storage of Special Access Program and SCI material in properly secured General Services Administration approved security containers within an accredited Special Access Program Facility.

Coalition

An arrangement between one or more nations for common action; multi-national action outside the bounds of established alliances, usually for single occasions or longer cooperation in a narrow sector of common interest; or a force composed of military elements of nations that have formed a temporary alliance for some specific purpose.

Critical Nuclear Weapon Design Information A DEPARTMENT OF DEFENSE category of weapon data designating TOP SECRET (Restricted Data) or SECRET (Restricted Data) revealing the theory

of operation or Design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition munitions, or test device.

Code Word

A code word is a single word assigned a classified meaning by appropriate authority to ensure proper security concerning intentions and to safeguard information pertaining to actual, real-world military plans or operations classified as confidential or higher.

Coercive Force

A negative or reverse magnetic force applied for the purpose of reducing magnetic flux density.

Coercivity

A property of magnetic material, measured in Oersteds, used as a measure of the amount of coercive force required to reduce the magnetic induction to zero from its remnant state. Generally used as a measure of the difficulty with which magnetic Information System storage devices can be degaussed.

Cognizant Security Agency

Agencies of the Executive Branch that have been authorized by Executive Order 12829, "National Industrial Security Program, to establish an industrial security program to safeguard classified information under the jurisdiction of those agencies when disclosed or released to U.S. Industry. These agencies are: DoD, Department of Energy (DOE), Office of the Director of National

Intelligence (ODNI), and the Nuclear Regulatory Commission (NRC).

Cognizant Security Office

The organizational entity delegated by the Head of a Cognizant Security Agency to administer industrial security on behalf of the Cognizant Security Agency. (Note: DSS has been designated by DoD Directive 5105.42 and DoD Instruction 5220.22 as the CSO for DoD.)

Cohabitant

A person with whom you share bonds of affection, obligation or other commitment, as opposed to a person with whom you live for reasons of convenience (a roommate).

Collateral Effect

Unintentional or incidental effects including, but not limited to, injury or damage to persons or objects that would not be lawful military targets under the circumstances ruling at the time. Includes effects on civilian or dual-use computers, networks, information, or infrastructure. Such effects are not unlawful as long as they are not excessive in light of the overall military advantage anticipated from the activity. In cyberspace operations, collateral effects are categorized as:

1. High: substantial adverse effects on persons or property that are not lawful targets from which there is a reasonable probability of loss of life, serious injury, or serious adverse effect on the affected nation's security, economic security, public safety, or any combination of such effects.

2. Medium: substantial adverse effects on persons or property that are not lawful targets.
3. Low: temporary, minimal or intermittent effects on persons or property that are not lawful targets.
4. No: only adversary persons and computers, computer-controlled networks, and/or information and information systems are adversely affected.

Collateral Information

Information classified at the Confidential, Secret, or Top Secret level. It does not include information subject to special access requirements such as (Sensitive Compartmented Information (SCI) or Special Access Programs (SAP).

Command Authority

The individual responsible for the appointment of user representatives for a department, agency, or organization and their key ordering privileges.

Command and Control Warfare

The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction. Command and control warfare is mutually supported by intelligence to deny information to, influence, degrade, or destroy adversary command and control capabilities. This process is accomplished while protecting friendly command and control capabilities against such actions. Command and control warfare applies across the operational continuum and all levels of conflict.

Commercial Off-The-Shelf

Commercial off-the-shelf or simply off the shelf is a term for software or hardware, generally technology or computer products, that are ready-made and available for sale, lease, or license to the general public. They are often used as alternatives to in-house developments or one-off government-funded developments. The use of Commercial off-the-shelf is being mandated across many government and business programs, as they may offer significant savings in procurement and maintenance. However, since Commercial off-the-shelf software specifications are written by external sources, government agencies are sometimes wary of these products because they fear that future changes to the product will not be under their control.

Communications Intelligence

Technical and intelligence information derived from the intercept of foreign communications by other than the intended recipients of those communications.

Communications Profile

An analytic model of communications associated with an organization or activity. The model is prepared from a systematic examination of communications content and patterns, the functions they reflect, and the Communications Security measures applied.

Communications Security

The protection resulting from all measures designed to deny unauthorized persons valuable information, which experts in electronics or telecommunications might be able to find. Some measures lead unauthorized persons to an incorrect interpretation of the information.

Community of Interest A restricted network of users, each having an Information System with an accredited security parameter identical to the others and having the need to communicate securely with other members of the network.

Community Risk

Probability that a particular vulnerability will be exploited within an interacting population and adversely impact some members of that population.

Company

A generic and comprehensive term for a business entity, which may be a sole proprietorship, partnership, corporation, society, association, limited liability company or other organization usually established and operating to carry out a commercial, industrial or other legitimate business, enterprise, or undertaking.

Compartmentation

A formal system for restricting access to selected activities or information. The establishment and management of an organization so that information about the personnel, internal organization, or activities of one component is

made available to any other component only to the extent required for the performance of assigned duties.

Compartmented Intelligence

National intelligence placed in a Director of National Intelligence-approved control system to ensure handling by specifically identified access approved individuals.

Compelling Need

A requirement for immediate access to special program information to prevent failure of the mission or operation or other cogent reasons.

Compromise Unauthorized disclosure of classified information.

Computer Network

The constituent element of an enclave responsible for connecting computing environments by providing short-haul data transport capabilities such as local or campus area networks, or long-haul data transport capabilities such as operational, metropolitan, or wide area and backbone networks.

Computer Network Attack (CNA)

Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

Computer Network Exploitation (CNE)

Enabling operations and intelligence collection

capabilities conducted through the use of computer networks to gather data from target or adversary information systems or networks. See also computer network attack.

Computer Security

Measures and controls that ensure confidentiality, integrity, and availability of information systems assets including hardware, software, firmware, and information being processed, stored, and communicated.

Computer Security Toolbox

A set of tools (BUSTER, FUSH, Secure Copy, etc.) designed specifically to assist Information Assurance Officer and System Administrators in performing their duties. The functions within the Toolbox can erase appended data within files; eliminate appended data in free or unallocated space; search for specific words or sets of words for verifying classification; and locating unapproved share programs. It also includes a program which allows you to clear laser toner cartridges and drums.

Computerized Telephone System

Also referred to as a hybrid key system, business communication system, or office communications system.

Computing Environment

Workstation or server (host) and its operating system, peripherals, and applications.

Communications Security Monitoring The act of listening to, copying, or recording transmissions of

one's own official telecommunications in order to analyze the degree of security.

Concealment

The act of remaining hidden.

Concept of Operations

A verbal or graphic statement, broadly outlining a commander's assumptions about or purpose of an operation or series of operations. The concept of operations frequently is embodied in campaign plans and operation plans; in the latter case, particularly when the plans cover a series of connected operations to be carried out simultaneously or in succession. The concept is designed to give an overall picture of the operation. It is included primarily for additional clarity of purpose. Frequently, it is referred to as commander's concept.

Confidential

The classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

Confidential Source

Any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

Confidentiality

The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information.

Configuration Control

Process of controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.

Configuration Management

The management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test fixtures, and test documentation of an information system, throughout the development and operational life of the system.

Connection Approval

Formal authorization to interconnect information systems.

Connectivity

A word which indicates the connection of two systems regardless of the method used physical connection.

Consignee

A person, firm, or government activity names as the receiver of a shipment; one to whom a shipment is consigned.

Consignor

A person, firm, or government activity by which articles are shipped. The consignor is usually the shipper.

Constant Surveillance Service

A transportation protective service provided by a commercial carrier qualified by Surface Deployment and Distribution Command to transport confidential shipments. The service requires constant surveillance of the shipment at all times by a qualified carrier representative; however, a Facility Security Clearance is not required for the carrier. The carrier providing the service must maintain a signature and tally record for the shipment.

Construction Surveillance Technician

A citizen of the United States, who is at least 18 years of age, cleared at the Top Secret level, experience in construction and trained in accordance with the Construction Surveillance Technician Field Guidebook to ensure the security integrity of a site.

Continental United States

United States territory, including adjacent territorial waters, located within the North American continent between Canada and Mexico.

Contingency Plan

Plan maintained for emergency response, backup operations, and post-disaster recovery for an information system, to ensure the availability of

critical resources and facilitate the continuity of operations in an emergency situation.

Continuous Operation

This condition exists when a Special Access Program Facility is staffed 24 hours every day.

Continuous Sensitive Compartmented Information Facility Operation

Staffing a Sensitive Compartmented Information Facility that is staffed and operated on a 24-hour a day, 7 days a week basis.

Contracting Officer

A government official who, in accordance with departmental or agency procedures, has the authority to enter into and administer contracts and make determinations and findings with respect thereto, or any part of such authority. The term also includes the designated representative of the contracting officer acting within the limits of his or her authority.

Contractor

Any individual or other legal entity that:

- (1) Directly or indirectly (e.g., through an affiliate), submits offers for or is awarded, or reasonably may be expected to submit offers for or be awarded, a Government contract, including a contract for carriage under Government or commercial bills of lading, or a subcontract under a Government contract; or
- (2) Conducts business, or reasonably may be expected to conduct business, with the

Government as an agent or representative of another contractor.

Contractor/Command Program Security Officer

An individual appointed at the contractor program facility to provide security administration and management based on guidance provided by the program Security Officer (PSO).

Contractor/Command Program Manager

A contractor-designated individual who has overall responsibility for all aspects of a Program.

Contractor Special Security Officer An individual appointed in writing by a cognizant security authority who is responsible for all aspects of Sensitive Compartmented Information security at a United States Government contractor facility.

Control

The authority of the agency that originates information, or its successor in function, to regulate access to the information.

Controlled Access Area

The complete building or facility area under direct physical control that can include one or more limited exclusion areas; controlled BLACK equipment areas, or in any combination.

Controlled Access Programs

Director of National Intelligence-approved programs that protect national intelligence. They include:

Sensitive Compartmented Information

Compartments that protect national intelligence concerning or derived from intelligence sources, methods, or analytical processes;

Special Access Programs

Pertaining to intelligence activities (including special activities, but excluding military, operational, strategic and tactical programs) and intelligence sources and methods; and

Restricted Collateral Information

Other than Sensitive Compartmented Information and Special Access Programs that imposes controls governing access to national intelligence or control procedures beyond those normally provided for access to Confidential, Secret, or Top Secret information, and for which funding is specifically identified.

Controlled Access Program Coordination Office

The Director of National Intelligence's focal point for issues dealing with the Controlled Access Program Oversight Committee and the Senior Review Group.

Controlled Access Program Oversight Committee

The forum supporting the Director of National Intelligence in the management of controlled access programs. This includes the creation and continuation of controlled access programs including Sensitive Compartmented Information compartments and other Director of National Intelligence special access programs. It

includes monitoring of these programs through performance audits and evaluations as necessary.

Controlled Area/Compound

Any area to which entry is subject to restrictions or control for security reasons.

Controlled Building

A building to which entry is subject to restrictions or control for security reasons.

Controlled Cryptographic Item

A secure telecommunications device, or information handling equipment ancillary device, or associated cryptographic component, that is unclassified but controlled. (Equipment and components so designed bear the designator "Controlled Cryptographic Item

Controlled Information

Information and indicators deliberately conveyed or denied to foreign targets in order to evoke invalid official estimates that result in foreign official actions advantageous to U.S. interests and objectives.

Controlled Interface

A mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system).

Controlled Unclassified Information

A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under

Executive Order 13526, but is:

- Pertinent to the national interests of the U.S. or to the important interests of entities outside the Federal Government; and
- Under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.

The designation CUI includes material marked “Sensitive But Unclassified” (SBU) and “For Official Use Only” (FOUO).

Cooperative Program Personnel

Foreign government personnel, assigned to a program office that is hosted by a Department of Defense Component in accordance with the terms of a Cooperative Program International Agreement, who report to and take direction from a Department of Defense -appointed program manager (or program manager equivalent) for the purpose of carrying out the cooperative project or program. Foreign government representatives described in such agreements as liaison officers or observers are not considered Cooperative Program Personnel and are treated as Foreign Liaison Officers.

Core Secrets

Any item, process, strategy, or element of information, the compromise of which would result in unrecoverable failure.

Corporate Family

The corporation, its subsidiaries, divisions and branch offices.

Corporation

A legal entity governed by a set of bylaws and owned by its stockholders.

Corroborate

To strengthen, confirm, or make certain the substance of a statement through the use of an independent, but not necessarily authoritative source. For example, the date and place of birth recorded in an official personnel file that could be used to corroborate the date and place of birth claimed on a Standard Form 86. See: "Verify".

Counterintelligence

That phase of intelligence covering all activity designed to neutralize the effectiveness of adversary intelligence collection activities.

Those activities that are concerned with identifying and counteracting the security threat posed by hostile intelligence services, organizations, or by individuals engaged in espionage, sabotage, subversion, or terrorism.

Counterintelligence Assessment

A Department of Defense Component's comprehensive analysis or study of a relevant Counterintelligence topic, event, situation, issue, or development. Counterintelligence assessments require exhaustive amounts of research and the production timeline can range from days to months. When conducted in support of a

Research, Development, and Acquisition program with Critical Program Information, the assessment describes the threat a foreign entity (person, representative, corporation, government, military, commercial, etc.) represents to the Critical Program Information/system assessed. The assessment is multidisciplinary as it includes an analysis of the diverse foreign collection modalities available, the relative effectiveness of each, and capability of the foreign entity to collect information about research efforts, the technology, and/or system under development. The assessment may include the impact to the Department of Defense if the technology is compromised and be complimentary to, integrated with, or independent of the Technology Targeting Risk Assessment provided by the Defense Intelligence Community.

Countermeasures

The employment of devices and/or techniques that has as its objective the impairment of the operational effectiveness of an adversary's activity. Countermeasures may include anything that effectively negates an adversary's ability to exploit vulnerabilities.

Courier

A cleared employee whose principal duty is to transmit classified material to its destination. The classified material remains in the personal possession of the courier except for authorized overnight storage.

Co-Utilization Agreement

Two or more organizations sharing the same Special Access Program Facility.

Cover

Protective action taken to mask or conceal an operation or activity from an adversary.

Covert Operation

An operation that is so planned and executed as to conceal the identity of, or permit plausible denial by, the sponsor. A covert operation differs from a clandestine operation in that emphasis is placed on concealment of the identity of the sponsor, rather than on concealment of the operation. Synonymous with law enforcement's undercover operation.

Credit Check

Information provided by credit bureaus or other reporting services to the credit history of the subject of a personnel security investigation.

Criminal Activity

Conduct that is or may be a violation of a federal or state criminal law, the Uniform Code of Military Justice, the common law, and the criminal laws of foreign countries that might embarrass or otherwise be of concern to the Department of Defense. Selective judgment should be exercised in determining what matters are to be reported based on such factors as the nature of the criminal act, the clearance level of the individual concerned, and his or her relative position in the company.

Critical and Sensitive Information List

Those areas, activities, functions, or other matters that a facility/organization considers most important to keep from adversaries.

Critical Design Review

A formal review conducted on each configuration item when design is complete. Determines that the design satisfies requirements, establishes detailed compatibility, assesses risk, and reviews preliminary product specifications.

Critical Information

Specific facts about friendly (e.g., U.S.) intentions, capabilities, or activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for accomplishment of friendly objectives.

Critical Infrastructures

Certain national infrastructures so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government.

Critical Nuclear Weapon Design Information

That TOP SECRET RESTRICTED DATA or SECRET RESTRICTED DATA revealing the theory of operation

or design of the components of a thermo-nuclear or implosion-type fission bomb, warhead, demolition munitions or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited life components; and total contained quantities of fissionable and high explosive materials by type. Among these excluded items are the components that Department of Defense personnel set, maintain, operate, test, or replace.

Critical Program Information

That information about the program, technologies, and/or systems that if compromised would degrade combat effectiveness or shorten the expected combat-effective life of the system. Access to this information could allow someone to kill, counter or clone the acquisition system before or near scheduled deployment or force a major design change to maintain the same level of effectiveness.

Cryptoanalysis

Operations performed in converting encrypted messages to plain text without initial knowledge of the crypto-algorithm and/or key employed in the encryption.

Crypto-Ignition Key

A device or electronic key used to unlock the secure mode of crypto equipment.

Cryptologic Information System

A Cryptologic Information System is defined as any Information System which directly or indirectly

supports the cryptologic effort, to include support functions, such as administrative and logistics, regardless of manning, location, classification, or original funding citation. This includes strategic, tactical, and support Information System: terrestrial, airborne, afloat, in-garrison, and space borne Information System; Information System dedicated to information handling; and information-handling portions of Information System that perform other functions.

Crypto-Equipment

The equipment used to render plain information unintelligible and restore encrypted information to intelligible form.

Cryptography

Art or science concerning the principles means, and methods for rendering plain information unintelligible and of restoring encrypted information to intelligible form.

Cryptology

The branch of knowledge that treats the principles of cryptography and cryptoanalytics; and the activities involved in producing signals intelligence and maintaining communications security.

Crypto-Security

The component of communications security that results from the providing and properly using technically sound cryptosystems.

Custodian

An individual who has possession of, or is otherwise charged with, the responsibility for safeguarding classified information.

Customer

The Government organization that sponsors the processing.

Cyber Attack

An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/ infrastructure; or destroying the integrity of the data or stealing controlled information.

Cyber Incident

Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. Synonymous with the term "Cyber Event."

Cyber Operational Preparation of the Environment

(C-OPE) Non-intelligence enabling functions within cyberspace conducted to plan and prepare for potential follow-on military operations. C-OPE includes but is not limited to identifying data, system/network configurations, or physical structures connected to or associated with the network or system (to include software, ports, and assigned network address ranges or other identifiers) for the purpose of determining system

vulnerabilities; and actions taken to assure future access and/or control of the system, network, or data during anticipated hostilities.

C-OPE replaces CNE or CNA when used specifically as an enabling function for another military operation.

Cyber-Security

The ability to protect or defend the use of cyberspace from cyber attacks.

Cyberspace

A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Cyberspace Operations (CO)

(CM-0856-09 1 Sep09). The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid.

Cyberspace Superiority

The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations of that force, and its related land, air, sea, and space forces at a given time and sphere of operations without prohibitive interference by an adversary.

Cyber Warfare (CW)

An armed conflict conducted in whole or part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict. It includes cyber attack, cyber defense, and cyber enabling actions.

Defensive Counter-cyber (DCC)

All defensive countermeasures designed to detect, identify, intercept, and destroy or negate harmful activities attempting to penetrate or attack through cyberspace. DCC missions are designed to preserve friendly network integrity, availability, and security, and protect friendly cyber capabilities from attack, intrusion, or other malicious activity by pro-actively seeking, intercepting, and neutralizing adversarial cyber means which present such threats. DCC operations may include: military deception via honeypots and other operations; actions to adversely affect adversary and/or intermediary systems engaged in a hostile act/imminent hostile act; and redirection, deactivation, or removal of malware engaged in a hostile act/imminent hostile act.

Designated Approving Authority Representative

official delegated by the Designated Approving Authority, as responsible for ensuring conformance to prescribed security requirements for components of sites under purview.

Damage

A loss of friendly effectiveness due to adversary action. Synonymous with harm.

Damage Assessment The analysis of the impact on national security of a disclosure of classified information to an unauthorized person.

Damage To The National Security

Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information.

Data

Information, regardless of its physical form or characteristics, that includes written documents, automated information systems storage media, maps charts, paintings, drawings, films photos, engravings, sketches, working notes, and sound, voice, magnetic, or electronic recordings in any form.

Data Integrity

The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction.

The property that data has not been exposed to accidental or malicious alteration or destruction.

DD 254 – Final

(Final DD254) – A Contract Security Classification Specification that is issued by a Government Contracting Activity or a Prime Contractor to extend retention authorization to contractors who wish to retain classified information beyond the terms of the contract as authorized by the National Industrial Security Program Operating Manual.

DD 254 – Original

(Original DD 254) –. An original DD 254 is issued during the solicitation phase of a classified contract to provide classification guidance and security requirements to prospective contractors/subcontractors as they formulate their bids. Once the contract is awarded, an original DD 254 is issued to the contractor /subcontractor awarded the classified contract.

Dead Bolt

A lock bolt with no spring action. Activated by a key or turn knob and cannot be moved by end pressure.

Deadlocking Panic Hardware

A panic hardware with a deadlocking latch that has a device when in the closed position resists the latch from being retracted.

Debriefing

The process of informing a person his need-to-know for access is terminated.

Deception

Those measures designed to mislead the enemy/adversary by manipulation, distortion, or falsification of evidence in order to induce a reaction from that adversary which is prejudicial to the adversary's interests.

Decibel

A unit of sound measurement.

Declassification

The determination that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure, together with removal or cancellation of the classification designation.

Declassification Authority

The official who authorized the original classification, if that official is still serving in the same position;

- The originators current successor in function;
- A supervisory official of either; or
- Officials delegated declassification authority in writing by the agency head or the senior agency official.

Declassification Guide

A guide providing classification and declassification instructions specifically for information that is 25 years old or older and of permanent historical value. A declassification guide is also the most commonly used vehicle for obtaining Interagency Security Classification Appeals Panel approval of 25-year exemptions from the automatic declassification provisions of Executive Order 13526, as amended.

Defense Articles

Any weapons, weapon systems, munitions, aircraft, boats, or other implements of war; any property, installations, commodities, materials, equipment, supplies, or goods used for the purposes of furnishing military assistance or

making military sales; any machinery, facility, tool, material, supply, or other item necessary for the manufacture, production, processing, repair, servicing, storage, construction, transportation, operation, or use of any other defense article; and any component or part of any articles listed above.

Defense Central Security Index

An automated sub-system of the Defense Central Index of Investigations designed to record the issuance, denial or revocation of security clearances, access to classified information, or assignment to a sensitive position by all Department of Defense Components for military, civilian, and contractor personnel. The Defense Central Security Index will serve as the central Department of Defense repository of security related actions in order to assist Department of Defense security officials in making sound clearance and access determinations. The Defense Central Security Index shall also serve to provide accurate and reliable statistical data for senior Department of Defense officials, Congressional committees, the General Accounting Office and other authorized Federal requesters.

Defense Central Index of Investigations

The Defense Central Index of Investigations is an automated Department of Defense repository that identifies investigations conducted by Department of Defense investigative agencies and personnel

security determinations made by Department of Defense adjudicative authorities.

Defense-in-Depth

Information Security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

Defense Industrial Security Clearance Office

A directorate of the Defense Security Service (DSS) which serves as the Central Adjudication Facilities (CAF) responsible, on behalf of the Department of Defense, for determining the personnel clearance eligibility of contractor employees requiring access to classified information; for maintaining personnel clearance records and furnishing information to authorized activities; for processing security assurances, clearances, and visits involving the United States and foreign countries; and for monitoring the cleared contractor's continued eligibility in the National Industrial Security Program (NISP).

Defense Information Infrastructure

Encompasses information transfer and processing resources, including information and data storage, manipulation, retrieval, and display. More specifically, the Defense Information Infrastructure is the shared or interconnected system of computers, communications, data, applications, security, people, training, and other support structure, serving the Department of Defense's local and worldwide information needs. The

Defense Information Infrastructure:

- connects Department of Defense mission support, command and control, and intelligence computers and users through voice, data, imagery, video, and multimedia services, and
- Provides information processing and value-added services to subscribers over the Defense Information systems Network. Unique user data, information, and user applications are not considered part of the Defense Information Infrastructure.

Defense Information systems Network

A sub-element of the Defense Information Infrastructure, the Defense Information systems Network is the Department of Defense's consolidated worldwide enterprise level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. It is transparent to its users, facilitates the management of information resources, and is responsive to national security and defense needs under all conditions in the most efficient manner.

The Defense Information systems Network is an information transfer network with value-added services for supporting national defense C3I decision support requirements and Classified Military Information functional business areas. As an information transfer utility, the Defense Information systems Network provides dedicated

point-to-point, switched voice and data, imagery and video teleconferencing communications services.

Defense Information systems Network Designated Approving Authority

One of four Designated Approving Authorities responsible for operating the Defense Information systems Network at an acceptable level of risk. The four Defense Information systems Network Designated Approving Authorities are the Directors of the Defense Information systems Agency, the Defense Intelligence Agency, the National Security Agency and the Director of the Joint Staff (delegated to the Joint Staff Director for Command, Control, Communications, and Computer Systems (J-6)).

Defense Office of Hearings and Appeals

The office responsible for making denial/revocation decisions for Department of Defense contractors.

Defense Personnel Exchange Program

A program under which military and civilian personnel of the Department of Defense and military and civilian personnel of the defense ministries and/or military services of foreign governments, in accordance with the terms of an international agreement, occupy positions with and perform functions for a host organization to promote greater understanding, standardization, and interoperability.

Defense Security Service

The Defense Security Service (DSS) is an agency of the Department of Defense (DoD) located in Quantico, Virginia with field offices throughout the United States. The Under Secretary of Defense for Intelligence provides authority, direction and control over DSS. DSS provides the military services, Defense Agencies, 24 federal agencies and approximately 13,000 cleared contractor facilities with security support services.

Defense Services

The furnishing of assistance (including training) to foreign persons, whether in the U.S. or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing, or use of defense articles; the furnishing to foreign persons of any technical data, whether in the U.S. or abroad; or military training of foreign units and forces, regular and irregular, including formal or informal instruction of foreign persons in the U.S. or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise, and military advice.

Defense Travel Briefing

Formal advisories that alert travelers to the potential for harassment, exploitation, provocation, capture, entrapment, terrorism, or criminal activity. These briefings include recommended courses of action to mitigate

adverse security and personal consequences and suggest passive and active measures to avoid becoming a target or inadvertent victim.

Defense Treaty Inspection Readiness Program

A security education and awareness program pertaining to arms control.

Degauss

To reduce the magnetization to zero by applying a reverse (coercive) magnetizing force, commonly referred to as demagnetizing.

To reduce the correlation between previous and present data to a point that there is no known technique for recovery of the previous data.

Degausser

An electrical device or handheld permanent magnet assembly that generates a coercive magnetic force for degaussing magnetic storage media or other magnetic material.

Degaussing (Demagnetizing) Procedure using an approved device to reduce the magnetization of a magnetic storage media to zero by applying a reverse (coercive) magnetizing force rendering any previously stored data unreadable and unintelligible.

Delegation of Disclosure Authority Letter

A letter issued by the appropriate Designated Disclosure Authority (normally Navy IPO) to a designated Department of Navy official defining classification levels, categories, scope, foreign countries, and limitations of information that may be authorized by the designated Department of

Navy official for disclosures to a foreign recipient. Under no circumstances may the contents of Delegation of Authority Letter be disclosed or acknowledged to foreign representatives. Delegations of Authority Letter's are general or subject-specific.

Deliberate Compromise of Classified Information

Any intentional act done with the object of conveying classified information to any person not officially authorized to receive it.

Demilitarized Zone

Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal network from outside attacks. A Demilitarized Zone is also called a "screened subnet."

Denial

The act of disowning or disavowing.

The refusal to grant something. See also deception; denial of service.

Denial of Service

When action(s) result in the inability to communicate and/or the inability of an Automated Information System or any essential part to perform its designated mission, either by loss or degradation of a signal or operational capability.

Department/Agency/Organization Code

A 6-digit identification number assigned by the Secure Telephone Unit /Secure Telephone Equipment Central Facility to organizational descriptions. The Department/Agency/Organization Code must be used by units when placing an order for Secure Telephone Unit /Secure Telephone Equipment keying material.

Department of Defense Component

Includes the Office of the Secretary of Defense; the Military Departments; Organization of the Joint Chiefs of Staff; Directors of Defense Agencies and the Unified and Specified Commands.

Department of Defense Information System

Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes Automated Information System applications, enclaves, outsourced Information Technology-based processes, and platform Information Technology interconnections.

Department of Defense National Agency Check Plus Written Inquires

A personnel security investigation conducted by the Defense Investigative Service for access to SECRET information consisting of a National Agency Check, credit bureau check, and written inquires to current and former employers (See paragraph 2, Appendix B), covering a 5-year scope.

Derivative Classification

The incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that applies to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification. Persons who apply derivative classification markings shall observe and respect original classification decisions and carry forward to any newly created documents any assigned authorized markings.

Derogatory Information

Information that could adversely reflect on a person's character, trustworthiness, loyalty, or reliability, for example, a history of drug abuse or criminal activity. Information that is unrelated to character (such as foreign connections) while of adjudicative significance, is not derogatory information. Generally derogatory information is characterized as follows:

- **Minor Derogatory Information:** Information that, by itself, is not of sufficient importance or magnitude to justify an unfavorable administrative action in a personnel security determination.
- **Significant Derogatory Information:** Information that could, in itself, justify, an unfavorable administrative action, or

prompt an adjudicator to Seek additional investigation or clarification.

Designated Approving Authority

The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with authorizing official, Designated Accrediting Authority and Delegated Accrediting Authority.

Designated Disclosure Authority

An official at a Department of Navy organization (e.g., command, agency, staff element) that has been granted a general delegation of disclosure authority by Navy International Programs Office and is responsible for controlling disclosures of Classified Military Information and Controlled Unclassified Information at that organization. Normally, the designated official is nominated by the head of his or her organization and is approved by Navy International Programs Office following the issuance of the general delegation of disclosure authority to the Department of Navy organization.

Designated Intelligence Disclosure Official

The heads of IC organizations or those United States Government Officials who have been designated by the Director of National Intelligence, in writing, as having the authority to approve or deny disclosure or release of unclassified intelligence information to foreign governments in accordance with applicable disclosure policies and procedures.

Dissemination

The provision of national intelligence to consumers in a form suitable for use.

Destroying

Destroying is the process of physically damaging the media to the level that the media is not usable, and that there is no known method of retrieving the data.

Detectable Actions

Physical actions or whatever can be heard, observed, imaged, or detected by human senses, or by active and/or passive technical sensors, including emissions that can be intercepted.

Determination Authority

A designee of a Senior Official of the Intelligence Community with responsibility for decisions rendered with respect to Sensitive Compartmented Information access eligibility or ineligibility.

Deviation

See: "Personnel Security - Exception"

Digraph and/or Trigraph

A two and/or three-letter acronym for the assigned Code Word or nickname.

Direction Finding

A procedure for obtaining bearings of radio frequency emitters by using a highly directional antenna and a display unit on an intercept receiver or ancillary equipment.

Directive

An authoritative decision from an official body, which may or may not have binding force.

Disclosure

The release of information through approved channels.

Disclosure Record

A record of names and dates of initial access to any Program information. (e.g. *exempli gratia*).

Discretionary Access Control

A means of restricting access to objects (e.g., files, data entities) based on the identity and need-to-know of subjects (e.g., users, processes) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).

Diskette

A metal or plastic disk, coated with iron oxide, on which data are stored for use by an Is. The disk is circular, rotates inside a square lubricated that allows the read/write head access to the disk.

Disposition

Disposition indicates that a matter, an item, or a concept has been satisfactorily completed. It can also mean a person's character traits, dealing mainly with the person's outlook on life.

Document

Any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

Documentary Information

Any information, which is recorded on paper, film, transparency, electronic medium, or any other medium. This includes, but is not limited to printed publications, reports, correspondence, maps, audiotapes, email, spreadsheets, databases and graphical slides, technical drawings, software code, and information embodied in hardware.

Downgrading

A determination that classified information requires, in the interest of national security, a lower degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect a lower degree of protection.

Drug Enforcement Administration

The Drug Enforcement Administration is a United States Department of Justice law enforcement agency tasked with combating drug smuggling and use within the U.S. Not only is the Drug Enforcement Administration the lead agency for domestic enforcement of the drug policy of the United States (sharing concurrent jurisdiction with the Federal Bureau of Investigation), it also has sole responsibility for coordinating and pursuing U.S. drug investigations abroad.

Dual Citizen

Any person who is simultaneously a citizen of more than one country.

Dual Technology

Passive Infra Red, microwave or ultrasonic Intrusion Detection System sensors which combine the features of more than one volumetric technology.

Economic Intelligence

Intelligence regarding economic resources, activities, and policies.

Electronic Intelligence

Technical and geo-location intelligence derived from foreign non-communications transmissions (e.g., radar) by other than nuclear detonations or radioactive sources.

Electronic Questionnaire for Investigative Processing

An Office of Personnel Management software program for the preparation and electronic submission of security forms for a personnel security or suitability investigation.

Electronic Security

Protection resulting from measures designed to deny unauthorized persons information from the interception and analysis of non-communication electromagnetic emissions.

Electronic Surveillance

Acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of the transmitter. Electronic surveillance may involve consensual interception of electronic communication and the use of tagging, tracking, and location devices. It should be noted that for the purpose of this

glossary, this definition is general, and more precise statutory definition may be found in Title 50 (Foreign Intelligence Surveillance Act).

Electronic Transmission

A transmission system that uses the flow of electric current (usually 4 - 20 milliamperes) to transmit output or input signals.

Electronic Warfare

Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are electronic attack, electronic protection, and electronic warfare support.

Eligibility

A determination that a person meets personnel security standards for access to Program material.

Emanation Security

Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by information systems. NOTE: This is also known as TEMPEST.

Emergency Action Plan

A plan developed to prevent loss of national intelligence; protect personnel, facilities, and communications; and recover operations damaged by terrorist attack, natural disaster, or similar events.

Emission Security

The component of Communications Security which results from all measures taken to deny unauthorized persons valuable information that might be derived from intercept and analysis of compromising emanations from crypto equipment and telecommunications systems.

Employee

A person, other than the President and Vice President, employed by, detailed or assigned to, an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head.

Enclave

Collection of information systems connected by one or more internal networks under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location.

Entrance National Agency Check

A personnel security investigation scoped and conducted in the same manner as a National Agency Check except that a technical fingerprint search of the files of the Federal Bureau of Investigation is not conducted.

Erasable Programmable Read-Only Memory

Abbreviation for Erasable Programmable Read-Only Memory. These devices are fabricated in much the same way as Erasable Programmable Read-Only Memory and, therefore, benefit from the industry's accumulated quality and reliability experience. As the name implies, erasure is accomplished by introducing electrical signals in the form of pulses to the device, rather than by exposing the device to ultraviolet light. Similar products using a nitride negative-channel metal-oxide semiconductor process are termed electrically alterable read-only memory.

Equity

Information originally classified by or under the control of an Agency.

Escort

A cleared person who accompanies a shipment of classified material to its destination. The classified material does not remain in the personal possession of the escort but the conveyance in which the material is transported remains under the constant observation and control of the escort.

Espionage

The act or practice of spying or of using spies to obtain secret intelligence.

Overt, covert, or clandestine activity. A term which is usually used in conjunction with the country against which such an activity takes place. For example, espionage against the United States.

Essential Elements of Friendly Information

In the context of “friend or foe,” these are specific pieces of information regarding friendly (i.e., our) intentions, capabilities, and activities which are likely to be sought by our foes (i.e., our enemies/competitors).

Essential Elements of Information

In the context of “friend or foe,” these are specific pieces of information which are likely to be sought by friendly planners about specific adversaries’ intentions, capabilities, and activities.

Essential Secrecy

The condition achieved by denial of critical information to adversaries.

Event

An observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring.

Exception

An adjudicative decision to grant or continue access eligibility despite a failure to meet adjudicative or investigative standards. Only the head of the agency concerned or designee will make such decisions. An exception precludes reciprocity without review of the case by the gaining organization or program. There are three types:

- Condition: Access eligibility granted or continued with the proviso that one or more additional measures will be required. Such measures include additional security

monitoring, restrictions on access and restrictions on an individual's handling of classified information. Submission of periodic financial statements, admonishment regarding use of drugs or excessive use of alcohol, and satisfactory progress in a government-approved counseling program is examples of conditions.

- **Deviation:** Access eligibility granted or continued despite either a significant gap in coverage or scope of investigation or an out-of-date investigation. "Significant gap" for this purpose means either a complete lack of coverage for a period of six months or more within the most recent five years investigated or the lack of an Federal Bureau of Investigation name or technical fingerprint check or the lack of one or more relevant investigative scope components (e.g. employment checks or a subject interview for an Single Scope Background Investigation, financial review for any investigation) in its entirety.
- **Waiver:** Access eligibility granted or continued despite the presence of substantial issue information that would normally preclude access. Agency heads or their designees approve waivers only when the benefit of access clearly outweighs any security concern raised by the shortcoming. A waiver may require special limitations on access, additional security monitoring and

other restrictions on the person's handling of classified information beyond normal need-to-know.

Executive Order

An order issued by the President to create a policy and regulate its administration within the Executive Branch.

Exempted

Nomenclature and marking indicating information has been determined to fall within an enumerated exemption from automatic declassification under Executive Order 13526, as amended.

Expanded National Agency Check

An Expanded National Agency Check consists of investigative inquiries (record reviews and/or interviews), as necessary, to determine if investigative issues are present or to substantiate or disprove unfavorable information disclosed during the conduct of an National Agency Check.

Expanded Steel

Also called EXPANDED METAL MESH. A lace work patterned material produced from 9/11 gauge sheet steel by making regular uniform cuts and then pulling it apart with uniform pressure.

Exploitation

The process of obtaining intelligence information from any source and taking advantage of it.

Export

The sending or taking a defense article out of the U.S. in any manner, except by mere travel outside

the U.S. by a person whose personal knowledge includes technical data; or, transferring registration or control to a foreign person of any aircraft, vessel, or satellite covered by the U.S. Munitions List, whether in the U.S. or abroad; or, disclosing (including oral or visual disclosure) or transferring in the U.S. any defense article to an embassy, any agency or subdivision of a foreign government (e.g., diplomatic mission); or, performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the U.S. or abroad.

Export License

The authorization issued by the State Department, Office of Defense Trade Controls, or by the Department of Commerce, Bureau of Industry and Security, which permits the export of International Traffic in Arms Regulations - or Export Administration Regulations - controlled articles, technical data, or services.

Export License Application

A request submitted by U.S. persons and foreign government entities in the U.S. to export International Traffic in Arms Regulations - or Export Administration Regulations - controlled technical data, services, or articles to a foreign person.

Extraordinary Security Measures

A security measure necessary to adequately protect particularly sensitive information but which imposes a substantial impediment to normal staff management and oversight. Extraordinary security

measures are:

- Program access nondisclosure agreements (read-on statements)
- Specific officials authorized to determine “need to know” (Access Approval Authority)
- Nicknames/codewords for program identification
- Special access required markings
- Program billet structure
- Access roster
- Use of cover
- Use of special mission funds or procedures
- Use of a Special Access Programs facility/vault
- Use of a dedicated Special Access Programs security manager
- Any other security measure beyond those required to protect collateral information.

Facilities

Buildings, structures, or other real property. Entities such as military bases, industrial sites, and office complexes may be identified as facilities.

Facility

A plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, that, when related by function and location, form an operating entity. (A business or educational organization may consist of one or more facilities as defined herein.) For purposes of industrial security, the term does not include Government installations.

Facilities Accreditation

An official determination of the physical, procedural and technical security acceptability of a facility that authorizes its use to protect classified national security information.

Facilities Certification

An official notification to the accreditor of the physical, procedural and technical security acceptability of a facility to protect classified national security information.

Facilities of Interest List

Not all listed Critical National Assets (CNA)
Critical Program Information (CPI) covered
Critical Infrastructure Program (CIP) Special
Access Program (SAP) already covered Foreign
Ownership Control Interest (FOCI) covered Arms

Ammunition and Explosives (AA&E) covered Trusted Foundries.

Facility Security Clearance

An administrative determination that, from a security viewpoint, a company is eligible for access to classified information of a certain category (and all lower categories).

Facility Security Officer

A U.S. citizen contractor employee, who is cleared as part of the facility clearance (FCL), responsible for supervising and directing security measures necessary for implementing applicable NISPOM and related Federal requirements for the protection of classified information.

Federal Personnel Manual

Manual issued and updated by Office of Personnel Management and designed to administer the personnel management of civilian employees of the Federal government.

Federal Record

Includes all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an Agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that Agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government

or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference, and stocks of publications and processed documents are not included. (44 United States Code 3301)

Ferroelectric Random Access Memory

Ferroelectric Random Access Memory is a type of non-volatile memory developed by Ramtron International Corporation. Ferroelectric Random Access Memory combines the access of speed of Dynamic Random Access Memory and Static Random Access Memory with the non-volatility of Read-only memory. Because of its high speed, it is replacing Electrically Erasable Programmable Read-Only Memory in many devices. The term Ferroelectric Random Access Memory itself is a trademark of Ramtron.

File Series

File units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.

Financial Crimes Enforcement Network

An activity of the Department of the Treasury that supports law enforcement investigative efforts and fosters interagency and global cooperation against domestic and international financial

crimes; it provides United States policymakers with strategic analyses of domestic and worldwide money laundering developments, trends and patterns. Financial Crimes Enforcement Network works toward those ends through information collection, analysis, and sharing, as well as technological assistance and implementation of the Bank Secrecy Act and other Department of Treasury authorities.

Financial Disclosure

A personnel security requirement for clearance processing that requires subjects to provide information regarding their total financial situation, e.g., assets, liabilities, and indebtedness.

Firewall

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

Fixed Disk

A magnetic storage device used for high volume data storage and retrieval purposes, which is not removable from the computer in which operates.

Flash Memory

A special type of Electrically Erasable Programmable Read-Only Memory that can be erased and reprogrammed in blocks instead of one byte at a time. Many modern personal computers have their Basic Input-Output System stored on a flash memory chip so that it can easily update if necessary. Such a Basic Input-Output System is sometimes called flash Basic Input-

Output System. Flash memory is also popular is modems because it enables the modern manufacturer to support new protocols as they become standardized. Flash memory is commonly used in Universal Serial Bus disk drives such as “Jump Drives”.

Flush

A computer program which is part of the Computer Security Toolbox. FLUSH is a Microsoft Disk Operating System based program used to eliminate appended data with a file or files and appended data located in unallocated or free space on a disk or diskette.

Foe

An opponent; the antithesis of friend.

Forced Entry

Entry by an unauthorized individual(s) that leaves evidence of the act.

For Official Use Only

Designation applied to unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act.

Foreign Contact

Contact with any person or entity that is not a United States citizen.

Foreign Disclosure

The disclosure of classified military information or controlled unclassified information to an authorized representative of a foreign government or international organization. The transfer or

disclosure of classified military information or controlled unclassified information to a foreign national who is an authorized employee of the U.S. Government or a U.S. contractor technically is not a “foreign disclosure,” since the disclosure is not made to the person’s government. For U.S. contractors, access by such persons will be handled under the provisions of the Arms Export Control Act or Export Administration Act and the National Industrial

Foreign Disclosure Point Of Contact

Foreign Disclosure Points Of Contact are Department of Navy officials who are appointed by the Chief of Naval Operations, the Commandant of the Marine Corps, Component Commanders, Commanders of Systems Commands, and the Chief of Naval Research for the coordination of foreign disclosure reviews and to facilitate a complete and timely response to foreign requests for classified military information or controlled unclassified information representing the consolidated organization position Foreign Disclosure Points Of Contact do not hold disclosure authority, unless also appointed as a Designated Disclosure Authorities.

Foreign Exchange Personnel

Military or civilian officials of a foreign defense establishment (i.e., a Department of Defense equivalent) who are assigned to a Department of Defense Component in accordance with the terms of an exchange agreement and who perform duties, prescribed by a position

description, for the Department of Defense Component.

Foreign Government Information

Information provided to the U.S. by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or, information produced by the U.S. pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

Foreign Intelligence

Information relating to the capabilities, intentions, and activities of foreign powers, organizations or persons, but not including counterintelligence except for information on international terrorist activities.

Foreign Intelligence Entity

An organization of a foreign government that engages in intelligence activities, per DoD 5240.06 (CI Awareness and Reporting).

Foreign Interest

Any foreign government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized, chartered or incorporated

under the laws of any country other than the U.S. or its possessions and trust territories, and any person who is not a citizen or national of the U.S.

Foreign Liaison Officer A foreign government military member or civilian employee authorized by his or her government and certified by a Department of Defense Component to act as an official representative of that government in its dealings with a Department of Defense Component in connection with programs, projects, or agreements of interest to that government. There are three types of Foreign Liaison Officers:

- **Security Assistance.** A foreign government representative who is assigned to a Department of Defense /Department of Navy Component or contractor facility in accordance with a requirement that is described in a Foreign Military Sales Letter of Offer and Letter of Acceptance.
- **Operational.** A foreign government representative who is assigned to a Department of Defense /Department of Navy Component in accordance with a documented requirement to coordinate operational matters, such as combined planning or combined exercises.
- **National Representative.** A foreign government representative who is assigned to his or her national embassy or delegation in the U.S. (e.g., an attaché) to conduct liaison activities with the Department of

Defense and the Department of Defense Components.

Foreign Military Sales

That part of security assistance authorized by the Arms Export Control Act and conducted using formal contracts or agreements between the U.S. Government and an authorized foreign purchaser. These contracts, called Letters of Offer and Acceptance are signed by both the U.S. Government and the purchasing Government or international organization and provide for the sale of defense articles and/or defense services (to include training) from Department of Defense stocks or through purchase under Department of Defense -managed contracts.

Foreign National

A person who is not a citizen or national of the United States.

Foreign Ownership, Control, or Influence

A Company is considered to be operating under Foreign Ownership, Control, or Influence whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts.

Foreign Person

A natural person who is not a lawful permanent resident as defined by 8 United States Code 1101 (a) (20), or who is not a protected individual as defined by 8 United States Code 1324b (a) (3). It also means any foreign corporation, business association, partnership, trust, society, or any other entity or group that is not incorporated or organized to do business in the U.S., as well as international organizations, foreign governments and any agency or subdivision of foreign governments (e.g., diplomatic missions).

Foreign Relations of the United States

The Foreign Relations of the United States series presents the official documentary historical record of major U.S. foreign policy decisions and significant diplomatic activity. The series, which is produced by the State Department's Office of the Historian, began in 1861 and now comprises more than 350 individual volumes. The volumes published over the last two decades increasingly contain declassified records from all the foreign affairs agencies.

Foreign Representative

A person, regardless of citizenship, who represents a foreign interest in his or her dealings with the U.S. Government, or a person who is officially sponsored by a foreign government or international organization. A United States national will be treated as a foreign person when acting as a foreign representative.

Foreign Travel Briefing

A security briefing given to a person with access to classified information who intends to travel outside the United States.

See: “Defensive Travel Briefing”

Foreign Visit

Any contact by a foreign representative with a Department of Navy organization or contractor facility. Such visits are of two types, based on sponsorship:

- Official Foreign Visit. Contact by foreign representatives under the sponsorship of their government or an international organization with a Department of Defense component or Department of Defense contractor facility. Only official visitors may have access to classified or controlled unclassified information.
- Unofficial Foreign Visit. Contact by foreign nationals with a Department of Defense / Department of Navy command or activity for unofficial purposes, such as courtesy calls and general visits to commands or events that are open to the public, or without sponsorship of their government. Such visitors shall have access only to information that has been approved for public disclosure.

Foreground Information

All information and material jointly generated and funded pertaining to the cooperative program. This information is available for use by all

participating governments in accordance with the terms of a Memorandum of Agreement.

Formerly Restricted Data

Information removed from the Restricted Data category upon a joint determination by the Department of Energy and the Department of Defense that such information related primarily to the military utilization of nuclear weapons and that such information can be safeguarded adequately as National Security Information (NSI) in the United States.

For Official Use Only Certified TEMPEST Technical Authority

An experienced, technically qualified U.S. Government employee who has met established certification requirements IAW the Committee in National Security Systems approved criteria and has been appointed by a United States Government Department or Agency to fulfill Certified Tempest Technical Authority responsibilities.

Freedom of Information Act

A provision that any person has a right, enforceable in court, of access to federal agency records, except to the extent that such records (or portions thereof) are protected from disclosure by one of nine exemptions.

Freight Forwarder (Transportation Agent)

Any agent or facility designated to receive, process, and transship U.S. material to foreign recipients. In the context of the DoD 5200.22-M,

NISPOM, an agent or facility cleared specifically to perform these functions for the transfer of U.S. classified material to foreign recipients.

Friend

In relation to national security, a country, individual, or organization with which one is allied in a struggle or cause.

Friendly

An adjective that describes an operation or activity that is carried out by a friend (e.g., friendly fire).

Gauss

A unit of measure of magnetic flux density.

General Services Administration

The General Services Administration is an independent agency of the United States government, established in 1949 to help manage and support the basic functioning of federal agencies. The GSA supplies products and communications for U.S. government offices, provides transportation and office space to federal employees, and develops government-wide cost-minimizing policies, among other management tasks. Its stated mission is to “help federal agencies better serve the public by offering, at best value, superior workplaces, expert solutions, acquisition services and management policies.”

Government Accounting Office

The Government Accountability Office is the audit, evaluation, and investigative arm of the United States Congress. It is located in the Legislative branch of the United States government. Its stated mission is: “the agency exists to support the Congress in meeting its constitutional responsibilities and to help improve the performance and ensure the accountability of the federal government for the benefit of the American people”.

Government-Approved Facility

Any Government owned room or outside of a Special Access Program Facility with controlled or restricted access designed to limit public access which has operational procedures in place to actually limit access; any Government owned Special Access Program Facility or area within a Special Access Program Facility.

Government Contracting Activity

An element of an agency designated by the agency head and delegated broad authority regarding acquisition functions.

Government-Off-The-Shelf

An item that has been developed by the government and produced to military or commercial standards and specifications, is readily available for delivery from an industrial source, and may be procured without change to satisfy a military requirement.

Government Program Manager

The senior Government Program official who has ultimate responsibility for all aspects of the Program.

Government-to-Government Transfer

The principle that classified information and material will be transferred by government officials through official government channels (e.g., military postal service, diplomatic courier) or through other channels expressly agreed upon in writing by the governments involved. In either case, the information or material may

be transferred only to a person specifically designated in writing by the foreign government as its designated government representative for that purpose.

Guard

A properly trained and equipped individual whose duties include the protection of a Special Access Program Facility. Guards will be United States citizens and with primary duty focus on the protection of US Government classified information. Guards will possess a United States SECRET clearance.

Guest System

Any system that enters the Special Access Program Facility which has not already been certified or accredited by the respective cognizant Special Access Program Facility authority is considered a Guest system.

Hacker

Unauthorized user who attempts to or gains access to an information system.

Hand carrier

A cleared employee who occasionally hand carries classified material to its destination in connection with a classified visit or meeting. The classified material remains in the personal possession of the hand carrier except for authorized overnight storage.

Handle Via Special Access Control Channels Only

A protective marking, (similar to For Official Use Only), used within Special Access Program control channels. It is used to identify CLASSIFIED or UNCLASSIFIED information which requires protection in Special Access channels. When Handle Via Special Access Channels Only is used to help identify classified Special Access Program information, the material will be protected in accordance with the security requirements of the individual Special Access Program or the highest standard where more than one Special Access Program is included.

Hard Disk

A magnetic storage device used for high volume data storage and retrieval purposes to include ones which are both removable and non-removable from the computers in which they operate.

Head of Department of Defense Component

The Secretary of Defense; the Secretaries of the Military Departments; the Chairman, Joint Chiefs of Staff; and the Commanders of Unified and Specified Commands and the Directors of Defense Agencies.

Home Office Facility

The headquarters facility of a multiple facility organization.

Human Intelligence

A category of intelligence derived from information collected and/or provided by human sources.

Hostile Act

Force or other means used directly to attach the US, US forces, or other designated persons or property, to include critical cyber assets, systems or functions. It also includes force or other means to preclude or impede the mission and/or duties of US forces, including the recovery of US personnel or vital US Government property.

Hostile Intent

The threat of an imminent hostile act. Determination of hostile intent in cyberspace can also be based on the technical attributes of an activity which does not meet the hostile act threshold but has the capability, identified through defensive counter cyber or forensic operations, to disrupt, deny, degrade, manipulate, and/or destroy critical cyber assets at the will of an adversary (such as a logic bomb or

'sleeper' malware). Because an individual's systems may be used to commit a hostile act in cyberspace without their witting participation, the standard for attribution of hostile act/intent for defensive counter-cyber purposes is 'known system involvement,' and is not witting actor or geography-dependent.

Illegal Drug Use

The use of drugs, possession or distribution of which is unlawful under the Controlled Substances Act. Such term does not include the use of a drug taken under the supervision of a licensed health care professional, other uses authorized by the Controlled Substances Act or other provisions of law.

Imagery

Collectively, the representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media.

Imagery Intelligence

Intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media.

Imitative Communications Deception

Introduction of deceptive messages or signals into an adversary's telecommunications signals.

Immediate Family Member

Mother, father, sister, brother, spouse, son, daughter. Each of these terms includes all its variants; e.g., "sister" includes sister by blood, sister by adoption, half-sister, stepsister, and foster sister. For purposes of determining access eligibility, cohabitants have a status identical to that of immediate family.

Immigrant Alien

Any alien lawfully admitted into the United States under an immigration visa for permanent residence.

Inadvertent Disclosure

A set of circumstances or a security incident in which a person has had involuntary access to classified information to which the individual was or is not normally authorized.

Incident

An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an IS; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Incident of Security Concern

Events that, at the time of occurrence, cannot be determined to be an actual violation of law, but which are of such significance as to warrant preliminary inquiry and subsequent reporting. Examples include drug use and distribution, alcohol abuse, the discovery or possession of contraband articles in security areas, and unauthorized attempts to access classified data.

Independent Research and Development

A contractor funded research and development effort that is not sponsored by, or required in performance of, a contract or grant that consists of projects falling within the areas of basic

research; applied research; development; and systems, and other concept formulation studies.

Indoctrination

An initial indoctrination and/or instruction provided each individual approved to a Special Access Program prior to his exposure concerning the unique nature of Program information and the policies, procedures, and practices for its handling.

Industrial Espionage

The act of Seeking a competitive, commercial advantage by obtaining a competitor's trade secrets and/or logistics. The acquisition of industrial information through clandestine operations.

Industrial Security

That portion of information security that is concerned with the protection of classified information in the custody of U.S. industry.

Information

Any knowledge, or documentary material, that may be communicated, regardless of its physical form or characteristics.

Information Assurance

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

Note: IS also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange systems,

and environmental control systems.

- **Information Assurance Certification and Accreditation:** The standard Department of Defense approach for identifying information security requirements, providing security solutions, and managing the security of Department of Defense information systems.
- **Information Assurance Control:** An objective Information Assurance condition of integrity, availability or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format, i.e., a control number, a control name, control text, and a control class. Specific management, personnel, operational, and technical controls are applied to each Department of Defense information system to achieve an appropriate level of integrity, availability, and confidentiality.
- **Information Assurance Product:** Product or technology whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control, non-repudiation of data); correct known vulnerabilities; and/or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks. Examples include such products as data/network encryptors, firewalls, and intrusion detection devices.

- Information Assurance -Enabled Information Technology Product: Product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security-enabled messaging systems.

Information Assurance Manager

The manager responsible for an organization's IS security program. Appointed by the Commander/Commanding Officer, or by company management in the case of a contractor. The Information Assurance Manager is the single point of contact for his/her organization concerning security matters to the Designated Approving Authority. The title of Information Assurance Manager replaced Information systems Security Manager.

Information Assurance Officer

The person responsible to the Information Assurance Manager for ensuring that operational security is maintained for specific Information System, sometimes referred to as a Network Security Officer, Terminal Area Security, or Information System Security Custodian. An Information Assurance Officer may have the responsibility for more than one system. The title of Information Assurance Officer replaced Information systems Security Officer.

Information Integrity

The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

Information Operation

Any action involving the acquisition, transmission, storage, or transformation of information that enhances the employment of military forces.

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 Security

The result of any system of administrative policies and procedures for identifying, controlling, and protecting information from unauthorized disclosure, the protection of which is authorized by executive order.

Information Security Oversight Office

The Information Security Oversight Office is responsible to the President of the United States for policy and oversight of the Government-wide security classification system and the National Industrial Security Program. Its authority derives from Executive Order 13526 "Classified National Security Information" and Executive Order 12829 "National Industrial Security Program", as amended.

The Information Security Oversight Office is a component of the National Archives and Records Administration and receives policy and program guidance from the National Security Council.

Information System

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

Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

Information systems Security

The 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 and Network Security

Information systems and network security is the protection afforded to Information systems in order to preserve the Availability, Integrity, and Confidentiality of the systems and the information contained with the system. Such protection is the integrated application of Communications Security, TEMPEST, and Information systems Security

executed in unison with personnel security, operations security, industrial security, resources protection, and physical security.

Information System Storage Device

The physical storage device used by an Information system upon which data is recorded.

Information System Security Engineer /System Design Security Officer

The individual responsible for the engineering process that captures and refines information protection requirements and ensures their integration into Information Technology acquisition processes through purposeful security design or configuration.

Information systems Security Representative

The Provider assigned individual responsibility for the onsite security of the Automated Information System, processing information for the Customer.

Information Warfare

Actions taken to achieve information superiority by adversely affecting an adversary's information, information-based processes, and/or information systems while defending one's own information, information-based processes, and/or information systems.

Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

Infraction

Any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not constitute a violation, as defined below.

Initial Operating Capability

A time when the person in authority (e.g. program/project managers of operations personnel) declares that a system meets enough requirements to formally be declared operational while the system may not meet all of the original design specifications to be declared fully operational.

Inspectable Space

A determination of the three-dimensional space surrounding equipment that processes classified and/or sensitive information within which TEMPEST exploitation is not considered practical, or where legal authority to identify and remove a potential TEMPEST exploitation exists.

Integral File Block

A distinct component of a file series, as defined in this section that should be maintained as a separate unit in order to ensure the integrity of the records. An integral file block may consist of a set of records covering either a specific topic or a range of time such as presidential administration or a 5-year retirement schedule within a specific file series that is retired from active use as a group.

Integrity

Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to the property whereby an entity has not been modified in an unauthorized manner.

Intelligence

The product from the collection, evaluation, analysis, integration, and interpretation of all available information, that concerns one or more aspects of foreign nations or of areas of foreign operations, and that is immediately or potentially significant to military planning and operations.

Intelligence Activity

An activity that an agency within the Intelligence Community is authorized to conduct under Executive Order 12333.

Intelligence Collection

The act of gathering information from all available sources to meet an intelligence requirement.

Intelligence Community

The aggregate of the following executive branch organizations and agencies involved in intelligence activities: the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; offices within

the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs; the Bureau of Intelligence and Research of the Department of State; intelligence elements of the military services, the Federal Bureau of Investigation, the Department of the Treasury, and the Department of Energy; and staff elements of the Office of the Director of Central Intelligence.

Intelligence Community Classification and Control Markings Implementation

A companion document to the Authorized Classification and Control Marking Register that provides guidance on the syntax and use of classification and control markings.

Intelligence Cycle

The steps by which information is converted into intelligence and made available to users. The cycle has been described as including five steps: planning and direction; collection; processing; production; and dissemination.

Intelligence Information

Unevaluated material that may be used in the production of intelligence.

Intelligence Sources and Methods

Sources: Persons, images, signals, documents, databases, and communications media capable of providing intelligence information through collection and analysis programs, e.g., Human Intelligence, Imagery Intelligence, Signal Intelligence, Geospatial, and Measurement and

Signature Intelligence; and

Methods: Information collection and analysis strategies, tactics, operations and technologies employed to produce intelligence products. If intelligence sources or methods are disclosed without authorization, their effectiveness may be substantially negated or impaired. (The term “intelligence sources and methods” is used in legislation and executive orders to denote specific protection responsibilities of the Director of National Intelligence.)

Intelligence Special Access Program

A Special Access Program established primarily to protect the planning and execution of especially sensitive intelligence or Counter Intelligence operations or collection activities.

Intelligence System

Any system (formal or informal) which is used to manage data gathering, obtain and process the data, interpret the data, and provide analytically-sound opinions to decision makers in order that they may make informed decisions with regard to various courses of action. The term is not limited to intelligence organizations or services but includes any system, in all its parts, that accomplishes the listed tasks.

Intending Citizen

An alien who falls into one of the following four categories under the Immigration Reform and Control Act of 1986.

Intention

An aim or design (as distinct from a capability) to execute a specified course of action.

Intercept

Data which is obtained through the passive collection of signals. Interrupting access, communication, or the flow of a process.

Interconnected Network

A network information system comprised of two or more separately accredited systems and/or networks.

Interim Access Authorization

A determination to grant access authorization prior to the receipt and adjudication of the individual's complicated background investigation.

See: "Temporary Access Eligibility"

Interim Approval to Operate

Temporary authorization granted by a Designated Approving Authority for an Information System to process classified information.

Interim Security Clearance

A security clearance based on the completion of minimum investigative requirements, which is granted on a temporary basis, pending the completion of the full investigative requirements.

Internal Vulnerability

The inside threat posed by an individual, with access to classified national intelligence, including

Sensitive Compartmented information, who may betray his or her trust.

See: "Insider Threat"

International Organization

An entity established by recognized governments under an international agreement which, by charter or otherwise, is able to acquire and transfer property, make contracts and agreements, obligate its members, and pursue legal remedies.

Interoperability

The capability of one system to communicate with another system through common protocols.

Intrusion Detection System

A security alarm system to detect unauthorized entry.

Invalidation

An administrative action that renders a contractor ineligible to receive additional classified information except that information necessary for completion of essential contracts as determined by appropriate Government Contracting Agencies.

Isolator

A device or assembly of devices which isolates or disconnects a telephone or Computerized Telephone System from all wires which exit the Special Access Program Facility and which has been accepted as effective for security purposes by the Telephone Security Group.

Issue Case

A case containing any issue information, even if fully mitigated.

Issue Information

See: “Personnel Security” – Issue Information

Joint Personnel Adjudication System

The centralized Department of Defense database of standardized personnel security processes; virtually consolidates the Department of Defense Central Adjudication Facilities by offering real time information concerning clearances, access, and investigative statuses to authorized Department of Defense security personnel and other interfacing organizations (e.g. Defense Security Service, Defense Manpower Data Center, Defense Civilian Personnel Management, and the Air Force personnel Center).

Joint Use Agreement

A written agreement signed by two or more accrediting authorities whose responsibility includes information processed on a common Automated Information System or network. Such an agreement defines a cognizant security authority and the security arrangements that will govern the operation of the network.

Joint Venture

A combination of two or more contractors without any actual partnership or corporation designation who perform or act jointly in a specific endeavor, such as the negotiation for or performance of a contract.

Key Material Identification Number

A unique number automatically assigned to each piece of Secure Telephone / Secure Telephone Equipment keying material by the Telephone / Secure Telephone Equipment.

Key Service Unit

An electromechanical switching device which controls routing and operation of an analog telephone system.

Laptop

See Portable Computer System.

Law Enforcement Sensitive

Law Enforcement Sensitive information is defined as unclassified information of a sensitive and proprietary nature that if disclosed could cause harm to law enforcement activities by jeopardizing investigations, compromising operations, or causing life-threatening situations for confidential informants, witnesses, or law enforcement personnel.

Lawful Permanent Resident

An individual having been lawfully accorded the privilege of residing permanently in the United States as an immigrant in accordance with the immigration laws, such status not having changed.

Lead

Single investigative element of a case requiring action. Leads include reference interviews, record checks, subject interviews, local agency checks, and national agency checks.

Letter of Compelling Need

A letter, signed by the Security Officer and Program Manager, used to justify or offset the risk related to accessing an individual who does not fully meet access criteria. The Letter of Compelling Need describes the benefit to the specific Special Access Program by describing the candidate's unique talent, particular expertise, or critically-needed skill.

Level of Concern

The Level of Concern is a rating assigned to an Information System by the Designated Approving Authority. A separate Level of Concern is assigned to each Information System for Confidentiality, Integrity and Availability. The Level of Concern for confidentiality, Integrity, and Availability can be Basic, Medium, or High. The Level of Concern assigned to an Information System for Confidentiality is based on the information it maintains processes and transmits. The Level of Concern assigned to an Information System for Integrity is based on the degree for resistance to unauthorized modifications. The Level of Concern assigned to an Information System for Availability is based on the needed availability of the information maintained, processed, and transmitted by the systems for mission accomplishment and how much too tolerance for delay is allowed.

Limited Access Authorization

Authorization for access to Confidential or SECRET information granted to non-United States citizens and immigrant aliens, which is limited to only that information necessary to the successful accomplishment of their assigned duties and based on a background investigation scoped for 10 years.

Limited Background Investigation

A Limited Background Investigation consists of a Personal Subject Interview; National Agency Check plus credit search; personal interviews with

employers (3 years), residence and educational sources (3 years); and law enforcement searches (5 years).

Limited Liability Company

Is a flexible form of enterprise that blends elements of partnership and corporate structures. It is a legal form of company that provides limited liability to its owners in the vast majority of United States jurisdictions. LLCs do not need to be organized for profit.

Line Supervision

Class I: Class I line security is achieved through the use of Data Encryption Standard or an algorithm based on the Cipher feedback or Cipher block chaining mode of encryption. Certification by National Institute of Science and Technology or another independent testing laboratory is required.

Class II: Class II line supervision refers to systems in which the transmission is based on pseudo random generated or digital encoding using an interrogation and response scheme throughout the entire communication, or Underwriter's Laboratory Class AA line supervision. The signal shall not repeat itself within a minimum six month period, Class II security shall be impervious to compromise using resistance, voltage, current, or signal substitution techniques.

Local Agency Check

An investigative check of local police departments, courts, etc., to determine whether

the subject has been involved in criminal conduct. The Local Agency Check is a part of all Personnel Security Investigation except Entrance National Agency Check.

Local Area Network

See: "Network"

Local Law Enforcement Check

See: "Local Agency Check"

Logic Bomb

A logic bomb is a program or code fragment which triggers an unauthorized, malicious act when some predefined condition occurs. The most common type is the "time bomb", which is programmed to trigger an unauthorized or damaging act long after the bomb is "set". For example, a logic bomb may check the system date each day until it encounters the specified trigger date and then executes code that carries out its hidden mission. Because of the built-in delay, a logic bomb virus is particularly dangerous because it can infect numerous generations of backup copies of data and software before its existence is discovered.

Long-Haul Telecommunications

All general purpose and special purpose long-distance facilities and services (including terminal equipment and local circuitry supporting the long-haul service) used to support the electromagnetic and/or optical dissemination, transmission, or reception of information via voice, data, video, integrated telecommunications, wire, or radio to

or from the post, camp, base, or station switch and/or main distribution frame (except for trunk lines to the first-serving commercial central office for local communications services). That includes Federal Telecommunications System 2000 , Digital Subscriber Network, Defense Data Network, the Automatic Digital Network, dedicated point-to-point service, and the primary inter-exchange carrier service associated with business or tie line to the local exchange carrier (e.g., Direct Distance Dialing, Foreign Exchange, Wide Area Telephone Service, 800 service, etc.) and contractor-provided telecommunications including the interconnection of various functional Information systems.

Low Probability of Detection

The result of measures used to hide or disguise intentional electromagnetic transmissions.

Low Probability of Intercept

Result of measures to prevent the intercept of intentional electromagnetic transmissions.

Letter of Intent

A letter from a Central Adjudication Facility to a subject, notifying of the Central Adjudication Facility's intent to deny/revoke security clearance/eligibility, and the reasons for the proposed action.

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.

Malicious Code Screening

Screening is the process of monitoring for the presence of malicious code. Malicious code occurs in different forms, which may have different methods for screening. Malicious code can arrive through either media that are introduced to Information System or as mobile code that arrives through connections to other systems and networks,

Mandatory Declassification Review

The review for declassification of classified information in response to a request for declassification that meets the requirements under sections 3.5, 3.6 of Executive Order 13526.

Manipulative Communications Deception

Alteration or simulation of friendly telecommunications for the purpose of deception.

Master Crypto-Ignition Key Custodian

An individual at each node in a Community of Interest who is responsible for controlling and maintaining the Master Crypto-Ignition Key and programming the security features of the Secure Terminal Equipment.

Material

Any product or substance on or in which information is embodied.

Measurement and Signature Intelligence

Scientific and technical intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic). This data is derived from specific technical sensors for the purpose of identifying any distinctive features associated with the source, emitter, or sender. This facilitates subsequent identification and or measurement of the same.

Memorandum of Agreement

A written agreement among relevant parties that specifies roles, responsibilities, terms, and conditions for each party to reach a common goal.

Memory Component

A memory Component is considered to be the Lowest Replaceable Unit in a hardware device. Memory components reside on boards, modules, and sub-assemblies. A board can be a module, or may consist of several modules and sub-assemblies.

Minimum Background Investigation

This investigation includes a National Agency Check and Inquiries, a credit record search, a face-to-face personal interview between the investigator and the subject, and telephone inquiries to selected employers.

A Minimum Background Investigation is typically reserved for public trust positions and/or when there is a break in federal service

Minor Derogatory Information

Information that, by itself, is not of sufficient importance or magnitude to justify an unfavorable administrative action in a personnel security determination.

Minor Issue Information

See: "Personnel Security"

Mission Assurance Category

Applicable to Department of Defense information systems, the mission assurance category reflects the importance of information relative to the achievement of Department of Defense goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories:

- Mission Assurance Category I. Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a Mission Assurance Category I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. Mission Assurance Category I

systems require the most stringent protection measures.

- Mission Assurance Category II. Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. Mission Assurance Category II systems require additional safeguards beyond best practices to ensure adequate assurance.
- Mission Assurance Category III. Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. Mission Assurance Category III systems require protective measures, techniques or procedures generally commensurate with commercial best practices.

Mission Essential

In the context of information, that information which is an essential portion of a unit's mandatory wartime capability.

Mitigation

(US CERT CONOPS, NRF) Solutions that contain or resolve risks through analysis of threat activity and vulnerability data which provide timely and accurate responses to prevent attacks, reduce vulnerabilities and fix systems. Activities providing a critical foundation in the effort to reduce the loss of life and property from natural and/or manmade disasters by avoiding or lessening the impact of a disaster and providing value.

Mobile Code

Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on local systems without explicit installation or execution by the recipient.

Modem

A device that electronically Modulates and Demodulates signals, hence the abbreviation MODEM.

Motion Detection Sensor

An alarm sensor that detects movement.

Multilevel Security

The concept of processing information with different classifications and categories that simultaneously permits access by users with

different security clearances and denies access to users who lack authorization.

Multiple Facility Organization

A legal entity (sole proprietorship, partnership, association, trust, corporation, or limited liability company) that is composed of two or more facilities.

Multiple Sources

Two or more source documents, classification guides, or a combination of both.

National Agency Check

A personnel security investigation consisting of a records review of certain national agencies including a technical fingerprint search of the files of the Federal Bureau of Investigation.

National Agency Check Plus Written Inquires

A personnel security investigation conducted by the office of Personnel Management, combining a National Agency Check and written inquiries to law enforcement agencies, former employers and supervisors, references and schools.

National Agency Check with Local Agency Checks and Credit Check

A personnel security investigation covering the past five to seven years and consisting of a National Agency Check , financial review, verification of date and place of birth, and local agency checks.

National Information Assurance Partnership

A U.S. Government program originally managed by the National Security Agency (NSA) to meet the security testing needs of both consumers and producers of IT.

National Information Infrastructure

The nation-wide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. It includes both public and private networks, the Internet, the public switched network, and cable, wireless, and satellite communications.

National Intelligence

All intelligence, regardless of the source from which derived and including information gathered within or outside the United States that (A) pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and (B) involves: (i) threats to the United States, its people, property, or interest; (ii) the development, proliferation, or use of weapons of mass destruction; or (iii) any other matter bearing on United States national or homeland security.

National of the United States

A citizen of the United States or a person who, though not a citizen of the United States, owes permanent allegiance to the United States.

National Military Strategy for Cyberspace Operations (NMS-CO)

The comprehensive strategy of the US Armed Forces to ensure US military superiority in cyberspace. The NMS-CO establishes a common understanding of cyberspace and sets forth a military strategic framework that orients and focuses DOD actions in the areas of military, intelligence, and business operations in and through cyberspace.

National Security Agency/Central Security Service

The Director, National Security Agency/Central Security Service is the authority for promulgation of computer security policy, and is also the PA for the security accreditation against that policy of

all IS and networks processing, using, storing, or producing cryptologic information.

National Security Information

Information that has been determined, pursuant to Executive Order 13526 or any predecessor order, to require protection against unauthorized disclosure, and that is so designated.

National Security-Related Information

Unclassified information related to national related to national defense or foreign relations of the United States.

Naval Nuclear Propulsion Information

Information, classified or unclassified, concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear-powered ships and prototypes, including the associated nuclear support facilities. Information concerning equipment, components, or technology which is applicable to both naval nuclear and conventional propulsion plants is not considered to be Naval Nuclear Propulsion Information when used in reference to conventional applications only, provided no association with naval nuclear propulsion can be directly identified from the information in question.

Need for Access

A determination that an employee requires access to a particular level of classified

information in order to perform or assist in a lawful and authorized governmental function.

Need-to-Know

A determination made by an authorized holder of classified information that a prospective recipient has a requirement for access to, knowledge, or possession of the classified information to perform tasks or services essential to the fulfillment of a classified contract or program.

Network

IS implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Network Manager

The individual who has supervisory or management responsibility for an organization, activity, or functional area that owns or operates a network.

Network Operations (NetOps)

(JP-1-02) Activities conducted to operate and defend the DOD's Global information Grid.

Network Security Officer

An Individual formally appointed by a Designated Approving Authority to ensure that the provisions of all applicable directives are implemented throughout the life cycle of an Information systems network. See also Information Assurance Officer.

Network System

A system that is implemented with collection of interconnected network components. A network system is based on a coherent security architecture and design.

Newly Discovered Records

Records that were inadvertently not reviewed prior to the effective date of automatic declassification because the Agency's declassification authority was unaware of their existence.

Nicknames

A combination of two separate unclassified words assigned to represent a specific Special Access Program or portion thereof.

Non-Conductive Section

Material (i.e. canvas, rubber, etc.) installed in ducts, vents, or pipes, and is unable to carry audio or radio frequency emanations.

Non-Discussion Area

A clearly defined area within a Special Access Program Facility where classified discussions are not authorized due to inadequate sound attenuation.

Non-Disclosure Agreement

An official authorized contract between an individual and the United States Government signed by an individual as a condition of access to classified national intelligence. It specifies the security requirements for access and details the penalties for noncompliance.

Non-Record Material

Certain documentary materials are specifically excluded by law (44 U.S.C. 3301) from the records of the Federal Government. Such materials are called "non-record." Any one or more of these three factors may determine whether something is a record or non-record: (1) the nature of the material; (2) the relationship to records; and (3) the use of the material.

Non-Repudiation

Assurance that the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so that neither can later deny having processed the data. Digital signatures are the current non-repudiation technique of choice for the National Information Infrastructure.

Nonvolatile Memory Components

Memory components that do retain data when all power sources are disconnected.

Notebook

See Portable Computer System.

Non-Volatile Random Access Memory

A type of memory that retains its contents when power is turned off. One type of Non-Volatile Random Access Memory is Static Random Access Memory that is made non-volatile by connecting it to a constant power source such as a battery. Another type of Non-Volatile Random Access Memory uses Electrically Erasable Programmable Read-only Memory chips to save its contents

when power is turned off. In this case, Non-Volatile Random Access Memory is composed of a combination of Static Random Access Memory and Electrically Erasable Programmable Read-only Memory chips.

North Atlantic Treaty Organization Classified Information

All classified information, military, political and economic circulated within North Atlantic Treaty Organization, whether such information originated in North Atlantic Treaty Organization or is received from member nations or from international organizations.

Object Reuse

The reassignment to some subject of a medium (e.g., page frame, disk sector, magnetic tape) that contained one or more objects. To be securely reassigned, such media will contain no residual data from the previously contained object(s).

Observables

Any actions that reveal indicators which are exploitable by adversaries.

Oersted

The unit of measure of a magnetic field.

Offensive Cyberspace Operations (OCO)

Offensive operations to destroy, disrupt, or neutralize adversary cyberspace capabilities both before and after their use against friendly forces, but as close to their source as possible. The goal of OCA operations is to prevent the employment of adversary cyberspace capabilities prior to employment. This could mean preemptive action against an adversary.

Office Information System

An Office Information System is a special purpose Automated Information System oriented to word processing, electronic mail, and other similar office functions. An Office Information System is normally comprised of one or more central processing units, control units, storage devices, user terminals, and interfaces to connect these components.

Office of Management and Budget

The federal agency that facilitates budget, policy, legislative, regulatory, and management issues on behalf of the President. The Office of Information and Regulatory Affairs within OMB develops policies to improve government statistics and information management, including statistical standards related to the collection of race and ethnicity data in the federal government.

Office of Personnel Management

One of the successor agencies to the Civil Service Commission. Office of Personnel Management conducts National Agency Check with Inquiries and Access National Agency Check and Inquiries on Department of Defense civilians and a broad range of Personnel Security Investigation for other federal agencies.

Official Department of Defense Information

All information that is in the custody and control of the Department of Defense, relates to information in the custody and control of the Department, or was acquired by Department of Defense employees as part of their official duties or because of their official status within the Department.

One Time Access

Access granted on a one-time basis to information classified one level higher than that of the current personnel security clearance.

Open Source Intelligence

Information of potential intelligence value that is available to the general public.

Open Storage Area

The storage of Special Access Program material within a Special Access Program Facility in any configuration other than within General Services Administration approved security containers

Operations Security

An analytic process used to deny an adversary information - generally unclassified –concerning intentions and capabilities by identifying, planning processes or operations. Operations Security does not replace other security disciplines – it supplements them. The Operations Security process includes the following five steps: (1) identify critical information, (2) identify the threat, (3) assess vulnerabilities, (4) analyze the risk, (5) develop and apply counter measures.

Operations and Support

A Special Access Program established to protect the planning for, execution of, and support to especially sensitive military operations. An operations and support Special Access Program may protect organizations, property, operational concepts, plans, or activities.

Operations Security Assessment

A thorough evaluation of the effectiveness of a customer's implementation of Operations Security methodology, resources, and tools. Assessments:

- Are used to evaluate the effectiveness of

the customer's corporate level Operations Security program and

- Can be used at the program level to determine whether or not a program is a viable candidate for an Operations Security survey.

Operations Security Indicator

Any detectable activity and/or information that, when looked at by itself or in conjunction with something else, allows an adversary to obtain critical or sensitive information.

Operations Security Plan

A strategy that analyzes an operation or activity and includes specific operations security measures.

Operations Security Process


An analytical process that involves five components: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Operations Security Program

An Operations Security program is the vehicle by which the principles and practices of Operations Security are employed within an organization.

Operations Security Survey

The application of Operations Security methodology at the program level. It is a detailed analysis of all activities associated with a specific operation, project or program in order to



determine what exploitable evidence of classified or sensitive activity could be acquired in light of the known collection capabilities of potential adversaries.

Operations Security Working Group

A (normally/formally) designated body representing a broad range of line and staff activities within an organization that provides Operations Security advice and support to leadership and all elements of the organization.

Optical Storage Media

Optical mass storage, including compact disks, optical disks, and magneto-optical disks.

Oral/Visual Disclosure

To brief orally, to expose to view, or to permit use under U.S. supervision in order to permit the transfer of knowledge or information, but not to physically transfer documents, material, or equipment to a foreign government or its representatives.

Organizational-level Commander/Commanding Officer

The individual, regardless of rank, who has been appointed as the officer-in-command of a physical organization.

Original Classification

An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of

protection required. (Only government officials who have been designated in writing may apply an original classification to information.)

Original Classification Authority

An individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance.


Originating Agency Determination Required

Declassification guidance for classified materials. Any material flagged Originating Agency Determination Required requires that the agency which originally classified the material determine whether the information can be declassified.

This was a popular declassification guidance during the Cold War. The use of Originating Agency Determination Required was halted by President William Jefferson Clinton in 1998. All documents with Originating Agency Determination Required guidance needed to have new guidance, or be declassified. Due to the non-existence of many originating agencies, many DOE nuclear secrets were almost declassified, until the order was modified.

Outsourced Information Technology based Process

For Department of Defense Information Assurance purposes, an outsourced Information Technology-based process is a general term used to refer to outsourced business processes supported by private sector information systems, outsourced



information technologies, or outsourced information services. An outsourced Information Technology-based process performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations.

Overseas Security Policy Board

The Board established by the President to consider, develop, coordinate and promote policies, standards and agreements on overseas security operations, programs and projects that affect all United States Government agencies under the authority of a Chief of Mission.

Overt Collection

The acquisition of information via the public domain.

Overt Operation

An operation conducted openly, without concealment.

Overwrite Procedure (for purposes of downgrading in limited cases)

Process which removes or destroys data recorded on an Information systems storage medium by writing patterns of data over, or on top of, the data stored on the medium.

Overwrite (Re-recording) Verification

An approved procedure to review, display, or check the success of an overwrite procedure. The successful testing and documentation through hardware and random hard-copy readout of the actual overwritten memory sectors.

Overwriting

A software process that replaces the data previously stored on magnetic storage media with a predetermined set of meaningless data. Overwriting is an acceptable method for clearing for release to environments of equal classification (Top Secret/Special Access Program to Top Secret/Special Access Program, Top Secret/Special Access Program to Top Secret/Sensitive Compartmented Information). However, the effectiveness of the overwrite procedure may be reduced by several factors: ineffectiveness of the overwrite procedures, equipment failure (E.G., misalignment of read/write heads), or inability to overwrite bad sectors or tracks or information in inter-record gaps. Software overwrite routines may be corrupted by the hostile computer viruses. Overwriting is not an acceptable method to declassify media.

Parent Corporation

A corporation that owns at least a majority of another corporation's voting securities.

Pass/Fail

A declassification technique that regards information at the full document or folder level. Any exemptible portion of a document or folder may result in exemption (failure) of the entire documents or folders. Documents or folders that contain no exemptible information are passed and therefore declassified. Documents within exempt folders are exempt from automatic declassification. Declassified documents may be subject to Freedom of Information Act exemptions other than the security exemption, and the requirements placed by legal authorities governing Presidential records and materials.

Pass Phrase

Sequence of characters, longer than the acceptable length of a password that is transformed by a password system into a virtual password of acceptable length.

Password

Protected/private character string used to authenticate an identity or to authorize access to data.

Password Shadowing

The ability with any operating system to physically store the password and/or encrypted password results in a mass storage area of the system other than in the actual password file itself. This feature

prevents the theft of passwords by hackers. Usually a UNIX feature.

Perceived Collection Threat

An estimate of the present and future resource allocations and capabilities of an adversary to gain information. Synonymous with potential threat.

Perimeter

The perimeter of an Automated Information System or network is the extent of the system that is to be accredited as a single system.

Periodic Reinvestigation

An investigation conducted every five years for the purpose of updating a previously completed background or special background investigation. The scope will consist of a personal interview, National Agency Check, Local Agency Check, credit bureau checks, employment records, employment references and developed character references and will normally not exceed the most recent five year period.

Periods Processing

The processing of various levels of classified and unclassified information at distinctly different times. Under the concept of periods processing, the system must be cleared of all information from one processing period before transitioning to the next. A system is said to operate in a "periods Processing" environment if the system is appropriately sanitized between operations in differing Protection Level periods, or with

differing user communities or data. Provided the sanitization procedures between each Protection Level segment have been approved by the Designated Approving Authority based on guidelines from the Program Manager(s) or responsible official(s), the system need meet only the security requirements of each processing period, while in that period. If the Designated Approving Authority approves the sanitization procedures for use between periods, the security requirements for a given period are considered in isolation, without consideration of other processing periods. Such sanitization procedures shall be detailed in the System Security Plans/System Security Authorization Agreement.

Peripheral

Any devices which are part of an Information System, such as printers, hard and floppy disk drives, and video display terminals.

Peripheral Devices

Any device attached to the network that can store, print, display, or enhance data (e.g., disk and/or tape, printer and/or plotter, an optical scanner, a video camera, a punched-card reader, a monitor, or card punch).

Permanent Resident Alien

Any alien lawfully admitted into the United States under an immigration visa for permanent residence.

Permanent Records

Any Federal record that has been determined by National Archives and Records Administration to have sufficient value to warrant its preservation in the National Archives of the United States.

Permanent records include all records accessioned by National Archives and Records Administration into the National Archives of the United States and later increments of the same records, and those for which the disposition is permanent on Standard Form 115s, Request for Records Disposition Authority, approved by National Archives and Records Administration on or after 14 May 1973.

Personal Computer System

A Personal Computer is a system based on a microprocessor and comprised of internal memory (Read Only Memory and Random Access Memory), input and/or output, and associated circuitry. It typically includes one or more read/write device(s) for removable magnetic storage media (e.g., floppy diskettes, tape cassettes, hard disk cartridges), a keyboard, Cathode Ray Tube or plasma display, and a printer. It is easily transported and is primarily used on desk tops for word processing, database management, or engineering analysis applications.

Personal Digital Assistants

These items are mint processors with computing power that are generally smaller than laptop, notebook, or palmtop computers. Some

examples include, but are not limited to, the Newton, Boss, Wizard, etc.

Personal Financial Statement

Form used as part of a personnel security investigation to provide a summary of a person's total monthly income, debt payments, expenses, and the net remainder of income.

Personal Identifiable Information

Information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

Personnel Security

A security discipline that assesses the loyalty, reliability and trustworthiness of individuals for initial and continued eligibility for access to classified information.

Personnel Security Clearance

An administrative determination that an individual is eligible, from a security viewpoint, for access to classified information at the same or lower category as the level of the personnel clearance being granted.

Personnel Security Determination

A discretionary security decision by appropriately trained adjudicative personnel of all available personal and professional information that bears on the individual's loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion and sound judgment, as well

as freedom from conflicting allegiances and potential for coercion, and the willingness and ability to abide by regulations governing the use, handling and protection of classified information and/or the execution of responsibilities of a sensitive position.

Personnel Security Exceptions

An adjudicative decision to grant or continue access eligibility despite a failure to meet all adjudicative or investigative standards. The head of the agency concerned or designee will make such decisions. (Exceptions with regard to eligibility for Sensitive Compartmented Information will be processed according to procedures established by the Director of National Intelligence). For purposes of reciprocity, the presence of an exception permits the gaining organization or program to review the case before assuming security sponsorship and to accept or decline sponsorship based on that review. When accepting sponsorship the gaining organization or program will ensure that the exception remains a matter of record. There are three types of exceptions: conditions, deviations, and waivers.

(1) *Conditions*: Access eligibility granted or continued with the provision that additional security measures shall be required. Such measures include, but are not limited to, additional security monitoring, access, restrictions, submission of periodic financial statements, and attendance at counseling sessions.

(2) *Deviations*: Access eligibility granted or continued despite either a significant gap in coverage or scope in the investigation or an out-of-date investigation. "Significant gap" for this purpose means either complete lack of coverage for a period of six months or longer within the most recent five years investigated or the lack of a Federal Bureau of Investigations name check or technical check or the lack of one or more relevant investigative scope components (e.g., employment checks, financial review, or a subject interview) in its entirety.

(3) *Waivers*: Access eligibility granted or continued despite the presence of substantial issue information that would normally preclude access. Agency heads or designees approve waivers only when the benefit of access clearly outweighs any security concern raised by the shortcoming. A waiver may require prescribed limitations on access such as additional security monitoring.

See: "Personnel Security"

Personnel Security Interview

An interview conducted with an application for or holder of a security clearance to discuss areas of security relevance. The term is also used to describe interviews with references in personnel security investigations.

Personnel Security Investigation

An investigation required for the purpose of determining the eligibility of Department of Defense military and civilian personnel, contractor

employees, consultants, and other persons affiliated with the Department of Defense, for access to classified information, acceptance or retention in the Armed Forces, assignment or retention in sensitive duties, or other designated duties requiring such investigation. Personnel Security Investigations include investigations of affiliations with subversive organizations, suitability information, or hostage situations, conducted for the purpose of making personnel security determinations. They also include investigations of allegations that arise subsequent to adjudicative action and require resolution to determine an individual's current eligibility for access to classified information or assignment or retention in a sensitive position.

Personnel Security – Issue Information

Any information that could adversely affect a person's eligibility for classified information. There are two types of issue information:

- (1) *Minor Issue Information*: Information that meets a threshold of concern set out in "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information", but for which adjudication determines that adequate mitigation, as provided by the Guidelines exist. Minor issue information does not provide the basis for waiver or condition.
- (2) *Substantial Issue Information*: Any information of aggregate of information that raises a significant question about the prudence of granting access eligibility. Substantial issue

information constitutes the basis for granting access eligibility with waiver or condition, or for denying or revoking access eligibility.

Personnel Security Program

The Department of Defense program established to ensure that only loyal, reliable and trustworthy people are granted access to classified information or allowed to perform sensitive duties.

Personnel Security Questionnaire

Security forms, whether paper or electronic, that are completed by a subject as part of a personnel security investigation. There are three versions of the Personnel Security Questionnaire: the Standard Form 85 for non-sensitive positions, the Standard Form 85P for public trust positions, and the Standard Form 86 for national security positions. See: "Questionnaire for National Security Positions"

Phased Periodic Reinvestigation

In September 2005 the Office of Personnel Management made the Phased Periodic Reinvestigation available as a less comprehensive and less expensive alternative to the Single Scope Background Investigation-Periodic Reinvestigation. The investigation includes a National Agency Check with Local Agency Checks and Credit Check, Personal Subject Interview, and limited reference interviews and record reviews. Phased Periodic Reinvestigations may not be requested when certain questions on the clearance application contain responses indicating a possible security or suitability issue.

Physical Security

The measures used to provide physical protection of resources against deliberate and accidental threats.

Physical Security Waiver

An exemption from specific standards for physical security for Sensitive Compartmented Information Facilities as outlined in Intelligence Community Directive

Palmtop

See Portable Computer System

Platform IT Interconnection

For Department of Defense Information Assurance purposes, platform Information Technology interconnection refers to network access to platform Information Technology. Platform Information Technology interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition, and operations. Platform Information Technology refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric. Examples of platform Information Technology interconnections

that impose security considerations include communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration.

Portable Computer System

Including Portable Electronic Devices and Portable Computing Device. Any computer system specifically designed for portability and to be hand carried by an individual (e.g., grids, laptops, cellular telephones, two-way pagers, palm-sized computing devices, two-way radios with functions including audio/video/data recording and/or playback featured, personal digital assistants, palm tops, notebooks, data diaries, and watches with communications software and synchronization hardware, etc.).

Portable Electronic Devices

Any non-stationary electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, personal digital assistants, pocket personal computers, palmtops, MP3 players, cellular telephones, video cameras, and pagers.

Portfolio

The aggregate of Information Technology investments for Department of Defense information systems, infrastructure and related technical activities that are linked to mission goals, strategies, and architectures, using various

assessment and analysis tools to permit information and Information Technology decisions to be based on their contribution to the effectiveness and efficiency of military missions and supporting business functions. Portfolios enable the Department of Defense to manage Information Technology resources and align strategies and programs with Defense-wide, functional, and organizational goals and measures.

Presidential Historical Materials and Records

The papers or records of the former Presidents under the legal control of the Archivist pursuant to sections 2107, 2111, 2111note, or 2203 of title 44, United States Code, as defined at 44 United States Code 2111, 2111note, and 2001.

Prime Contract

A contract let by a Government Contracting Activity to a contractor for a legitimate government purpose.

Prime Contractor

The contractor who receives a prime contract from a Government Contracting Activity.

Principal Accrediting Authority

The senior official having the authority and responsibility for all Information systems within an agency.

Principal Disclosure Authority

The Principal Disclosure Authority over sees compliance with Department of Navy disclosure

policy and is the only Department of Navy official other than the Secretary or Under Secretary of the Navy who is authorized to deal directly with the Secretary or Under Secretary of Defense regarding such matters as Department of Navy requests for exceptions to the National Disclosure Policy. The Principal Disclosure Authority for the Department of Navy is the Assistant Secretary of the Navy for Research.

Privacy (Not Security)

The rights of an individual or organizations to determine for themselves when, how, and to what extent information about them is transmitted to others.

Privileged User

A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Profile

A collection and/or display (e.g., a written or graphical description) of the signatures and patterns of an individual or organization.

Program Access Request

A formal request used to nominate an individual for Program access.

Program Channels or Program Security Channels

A method or means expressly authorized for the handling or transmission of classified or unclassified Special Access Program information whereby the information is provided to indoctrinated persons.

Program Executive Office, Enterprise Information systems

The Program Executive Office is responsible for developing, acquiring, and deploying tactical and non-tactical Information Technology systems and communications for the Army (examples include transportation, medical, personnel, and supply automated tracking and communications systems).

Program Executive Agent

The highest ranking military or civilian individual charged with direct responsibility for the Program and usually appoints the Government Program Manager.

Program Material

Program material and information describing the service(s) provided, the capabilities developed, or the item(s) produced under the Special Access Program.

Program Office

The office that manages, executes, and controls a Special Access Program in a Department of Defense component.

Program Protection Plan

A comprehensive protection and technology control management tool established for each defense acquisition program to identify and protect classified and other sensitive information from foreign intelligence collection or unauthorized disclosure.

Program Security Officer

The Government official who administers the security policies for the Special Access Program.

Program Sensitive Information

Unclassified information that is associated with the Program. Material or information that, while not directly describing the Program or aspects of the Program, could indirectly disclose the actual nature of the Program to a non-Program-briefed individual.

Project/Program Manager

The single individual responsible for a project or program who manages all day-to-day aspects of the project or program.

Programmable Read-Only Memory

Programmable Read-Only Memory is a memory chip on which data can be written only once. Once a program has been written onto a Programmable Read-Only Memory, it remains there forever. Unlike Random Access Memory, Programmable Read-Only Memory retains their contents when the computer is turned off. The difference between a Programmable Read-Only Memory and a Read-Only Memory is that a Programmable Read-Only is manufactured as blank memory, whereas a Read-Only Memory is programmed during the manufacturing process. To write data onto a Programmable Read-Only Memory chip, you need a special device called a Programmable Read-Only Memory programmer or Programmable Read-Only Memory burner. The

process of programming a Programmable Read-Only Memory is sometimes called burning the Programmable Read-Only Memory. An Erasable Programmable Read-Only Memory is a special type of Programmable Read-Only Memory that can be erased by exposing it to ultraviolet light. Once it is erased, it can be rewritten.

Proprietary Information

Material and information relating to, or associated with, a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and know-how that have been clearly identified and properly marked by the company as proprietary information, trade secrets, or company confidential information. The information must have been developed by the company and not be available to the government or to the public without restriction from another source.

Protected Distribution System

A wireline or fiber-optic telecommunications system that includes terminals and adequate acoustic, electrical, electromagnetic, and physical safeguards to permit its use for the unencrypted transmission of classified information.

Protected Information

Includes sensitive, critical and/or classified information.

Protective Measures

Those actions, procedures, or designs implemented to safeguard protected information.

Protective Security Service

A transportation protective service provided by a cleared commercial carrier qualified by the SCCD (Military Surface Deployment and Distribution Command), to transport SECRET shipments.

Protocols

Set of rules and formats, semantic and syntactic, that permits entities to exchanged information.

Provider

The Contractor or Government support organization (or both) that provides the process on behalf of the Customer.

Proxy

Software agent that performs a function or operation on behalf of another application or system while hiding the details involved. Typical proxies accept a connection from a user, make a decision as to whether or not the user or client network address is authorized to use the requested service, optionally perform additional authentication, and then complete a connection on behalf of the user to a remote destination.

Psychological Operations

Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and, ultimately, the behavior of foreign governments, organizations, groups, and individuals. The purpose of Psychological Operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.

Public Domain

In open view; before the public at large and not in private or employing secrecy or other protective measures.

Public Domain Software

Software not protected by copyright laws of any nation that carries no warranties or liabilities, and may be freely used without permission of or payment to the creator.

Public Information

Official Department of Defense information that has been reviewed and approved for public release by the information owner.

Purging

The removal of data from an Information systems, its storage devices, or other peripheral devices with storage capacity in such a way that the data may not be reconstructed. Note: An Information systems must be disconnected from any external network before a purge. See Sanitization.

Questionnaire for National Security Positions

The Standard Form 86 developed by the Office of Personnel Management for background investigations and reinvestigations. Completed by the applicant, the Questionnaire for National Security Positions provides details on various aspects of the individual's personal and professional background.

Random Procurement

Method of acquiring, from existing local off-the-shelf stock, by Top Secret cleared United States citizens, materials for use in new construction or modification to an existing Sensitive Compartmented Information Facility or secure work area. Procurement of material will be unannounced, made without referral and immediately transported by the procurer to a Secure Storage Area. Random procurement may also be used for the acquisition of equipment, material, or supplies to be used in a Sensitive Compartmented Information Facility or secure area.

Random Selection

The process of selecting a portion of building materials from a bulk shipment, procured for non-specific general construction use. Not authorized for Sensitive Compartmented Information Facilities or Secure Work Areas.

Reciprocity

Recognition and acceptance, without further processing of: (1) security background investigations and clearance eligibility determinations. (2) accreditations of information systems; and (3) facility accreditations. Reciprocity is obligatory in the IC when there are no waivers, conditions, or deviations to the Director of National Intelligence.

Records

The records of an agency and Presidential papers or Presidential records, as those terms are defined in title 44, United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant.

Records Having Permanent Historical Value

Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently in accordance with title 44, United States Code.

Records Management

The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

Recycled

Recycled is the end state for Information System storage devices processed in such a way as to make them ready for reuse to adapt them to a new use, or to reclaim constituent materials of value (i.e. smelting).

RED

A designation applied to telecommunications and Information System, plus associated areas, circuits, components, and equipment which, when classified plain text signals are being processed therein, require protection during electrical transmission.

RED/BLACK Concept

Separation of electrical and electronic circuits, components, equipment, and systems that handle classified plain text (RED) information, in electrical signal form, from those which handle unclassified (BLACK) information in the same form.

Redaction

For purposes of declassification, the removal of exempted information from copies of a document.

Reference

A person other than the subject of a background investigation, identified as having knowledge of the subject. References are characterized by source and type. There are two **sources**: listed (meaning the subject of the investigation identified the reference on the Personnel Security Questionnaire) and developed (meaning an investigator, in the course of pursuing leads, identified the reference as someone knowledgeable of the subject). There are six **types**: education (a faculty member or school administrator at a school attended by the subject who had knowledge of the subject when a

student), employment/supervisor (a person with management responsibilities for the subject), co-worker (a colleague with knowledge of the subject's on-the-job behavior), neighborhood (a person living in the subject's neighborhood who has knowledge of the subject), friend/associate (a person knowing the subject socially, preferably away from both work and home), knowledgeable person (a person who knows the subject in some other context; for example: a banker or attorney or real estate agent who conducts business on behalf of the subject; or a clerk in a store where the subject shops frequently). A specific reference can be categorized as more than one type: for example, someone who is both an office mate and fellow member of a softball team may be both a co-worker reference and a friend/associate reference.

Reference Material

Documentary material over which the Government Contracting Activity, who lets the classified contract, does not have classification jurisdiction, and did not have classification jurisdiction at the time the material was originated. Most material made available to contractors by the Defense Technical Information Center and the other secondary distribution agencies is reference material as thus defined.

Regrade

To raise or lower the classification assigned to an item of information.

Reinstatement

A process whereby a person whose access authorization has been terminated or revoked is permitted to again have access to classified information.

Release

Providing classified information in writing, or any other medium, for retention.

See: "Disclosure"

Remote Maintenance

An operational procedure that involves connection of a system to an external (i.e., outside of the facility securing the system), remote service for analysis or maintenance.

Remote Terminal

A device for communication with an automated information system (AIS) from a location that is not within the central computer facility.

Removable Hard Disk

A hard disk contained in a removable cartridge type casing.

Report of Investigation

Report of the results of investigative inquiries. All Personnel Security Investigations and results from criminal and counterintelligence agencies are Report of Investigations.

Representative of a Foreign Interest

A citizen or national of the U.S. who is acting as a representative of a foreign government,

an agency of a foreign government, or a representative of a foreign government.

Research and Technology

Activities that may be described as basic research, applied research, and advanced technology development, demonstrations or equivalent activities, regardless of budget activity. Definitions for Basic Research, Applied Research and Advanced Technology Development are provided in the Department of Defense, Financial Management. Regulation, Chapter 5.

Response Force

Personnel (not including those on fixed security posts) appropriately equipped and trained, whose duties include initial or follow up response to situations which threaten the security of the Special Access Program Facility. This includes local law enforcement support or other external forces as noted in agreements.

Restricted Area

A controlled access area established to safeguard classified material, that because of its size or nature, cannot be adequately protected during working hours by the usual safeguards, but that is capable of being stored during non-working hours in an approved repository or secured by other methods approved by the Cognizant Security Agency (DoD 5220.22-M, NISPOM)

Restricted Data

All data concerning design, manufacture or use of atomic weapons; the production of special

nuclear material; or, the use of special nuclear material in the production of energy, but not including data declassified or removed from the Restricted Data category pursuant to the Atomic Energy Act of 1954, as amended.

Revocation

An adjudicative decision to permanently withdraw an individual's clearances based on a personnel security investigation, other relevant information, or both, that a cleared person is no longer eligible for access to classified information.

Revocation of Facility Security Clearance

Administrative action that is taken to terminate all classified activity of a contractor because the contractor refuses, is unwilling, or has consistently demonstrated an inability to protect classified information.

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:

- (1) the adverse impacts that would arise if the circumstance or event occurs; and
- (2) the likelihood of occurrence.

Note: IS-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or IS and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Risk Analysis

A method by which individual vulnerabilities are compared to perceived or actual security threat scenarios in order to determine the likelihood of compromise of critical information.

Risk Assessment

Process of analyzing threats to, and vulnerabilities of, an IT system, and the potential impact that the loss of information or capabilities of a system would have on national security. The resulting analysis is used as a basis for identifying appropriate and effective measures.

Risk Avoidance

A security philosophy which postulates that adversaries are all-knowing and highly competent, against which risks are avoided by maximizing defenses and minimizing vulnerabilities.

Risk Management

The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation resulting from the operation or use of IS, and includes:

- (1) the conduct of a risk assessment;
- (2) the implementation of a risk mitigation strategy;
- (3) employment of techniques and procedures for the continuous monitoring of the security state of the information system; and
- (4) documenting the overall risk management program.

Robustness

The ability of an IA entity to operate correctly and reliably across a wide range of operational conditions, and to fail gracefully outside of that operational range. The Department of Defense has three levels of robustness:

- **High Robustness:** Security services and mechanisms that provide the most stringent protection and rigorous security countermeasures.
- **Medium Robustness:** Security services and mechanisms that provide for layering of additional safeguards above good commercial practices.
- **Basic Robustness:** Security services and mechanisms that equate to good commercial practices.

Routine Changes

Changes which have a minimal effect on the overall TEMPEST security of the Special Access Program Facility. Adding a different type electronic information processing equipment (unless the equipment added is known to have an unusually large TEMPEST profile), movement of the equipment with the facility, and minor installation changes are examples of routine changes.

Reimbursable Suitability Investigation

Focused investigation to provide additional specific information to resolve developed issues.

Sabotage

The willful destruction of government property with the intent to cause injury, destruction, defective production of national defense, or war materials by either an act of commission or omission.

Safeguarding and Safeguarding Measures

Controls that are prescribed to protect classified information.

Sanitization (Also Purging)

The actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.

Sanitizing

The removal of information from the media or equipment such that data recovery using any known technique or analysis is prevented. Sanitizing shall include the removal of data from the media, as well as the removal of all classified labels, markings, and activity logs. Properly sanitized media may be subsequently declassified upon observing the organization's respective verification and review procedures.

Special Access Program Central Office

Office within DoD or military department responsible for establishment and application of regulations, oversight, and security policy for Special Access Programs.

Scattered Castles

The Intelligence Community security clearance repository and the Director of National

Intelligence's authoritative source for clearance and access information for all Intelligence Community, military services, Department of Defense civilians, and contractor personnel. Department of Defense information is furnished by Joint Personnel Adjudication System.

Scheduled Records

All records that fall under a National Archives and Records Administration approved records control schedule are considered to be scheduled records.

Scope

The time period to be covered and the sources of information to be contacted during the prescribed course of a Personnel Security Investigation.

Sealed Disk Drive

See "Hard Disk"

Secret

The classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

Secure Copy

A computer program which is part of the Computer Security Toolbox. Secure Copy is a Microsoft-Disk Operating System based program used to eliminate appended data within a file or files while transferring the same from a source disk or diskette to a target disk or diskette.

Secure Data Device

The Secure Data Device provides a simple and cost-effective way to protect classified Government data transmissions. The Secure Data Device provides Secure Telephone Unit-III/STE secure data transmission functions without voice features and is fully interoperable with all other Secure Telephone Unit-III/STE products. It allows the user to access a computer database, send a FAX message, or use email and be sure the information is protected. The Secure Data Device was developed under the U.S. Government's Secure Telephone Unit-III/STE program and is approved for use by Federal department, agencies, and Government contractors.

Secure Telephone Unit III

The Secure Telephone Unit-III family includes several interoperable terminals capable of transmitting voice and data through the public telephone network. The Secure Telephone Unit-III can be used as an ordinary telephone, and can also be used as a secure terminal, connected through the public telephone network to other Secure Telephone Unit-III's. A Secure Telephone Unit-III provides Secure Telephone Unit-III secure data transmissions functions without voice features. Secure Telephone Unit-III's are endorsed by the National Security Agency for protecting classified or sensitive, unclassified U.S. Government information, when appropriately keyed.

Secure Terminal Equipment (STE)

Is the U.S. Government's current, encrypted

telephone communications system for wired or “landline” communications.

Secure Working Area

An accredited facility or area that is used for handling, discussing and/or processing, but not storage of Special Access Program information.

Security

A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.

Security Assurance

The written confirmation requested by and exchanged between governments, of the security clearance level or eligibility for clearance, of their employees, contractors and citizens. It includes a statement by a responsible official of a foreign government that the original recipient of U.S. classified information possesses the requisite security clearance and is approved by his or her government for access to information of the security classification involved on behalf of the foreign government and that the recipient will comply with any security requirements specified by the U.S. In the case of contractors, the security assurance includes a statement concerning the level of storage capability.

Security Classification Guides

Security Classification Guides are issued for each system, plan, program or project in which classified information is involved.

Security Clearance

A determination that a person is eligible, under the standards of this regulation, for access to classified information.

Security Cognizance

This is the responsibility assigned to CSAs to discharge industrial security responsibilities described in the NISPOM and other NISP-related issuances.

Security Compromise

The disclosure of classified information to persons not authorized access thereto.

Security Countermeasures

Actions, devices, procedures, and/or techniques to reduce security risk.

Security Director

Senior individual that is responsible for the overall security management of Special Access Program within that activity.

Security Domain

Within an information system, the set of objects that is accessible. Access is determined by the controls associated with information properties such as its security classification, security compartment or sensitivity. The controls are applied both within the information system and

in its connection to other classified or unclassified information systems.

Security Environment Changes

Changes which have a detrimental effect on the facility. Changes to the inspectable space, addition of a radio transmitter or a modern for external communications, removal or reduction of an existing TEMPEST countermeasure (Radio Frequency Interference Shielding, Filters, Control/ Inspectable space, etc.) would be changes to the security environment.

Security Environment Threat List

A list of countries with United States Diplomatic Missions that is compiled by the Department of State and updated semi-annually. The listed countries are evaluated based on: transnational terrorism; political violence; human intelligence; technical threats; and criminal threats. The following four threat levels are based on these evaluations:

Critical – defined as a definite threat to United States assets based on adversary's capability, intent to attack, and targeting conducted on a recurring basis;

High – defined as a credible threat to United States assets based on knowledge of an adversary's capability, intent to attack, and related incidents at similar facilities;

Medium – defined as a potential threat to United States assets based on knowledge of an adversary's desire to compromise the assets and

the possibility that the adversary could obtain the capability to attack through a third party who has demonstrated such a capability;

Low – defined as little as no threat as a result of the absence of credible evidence of capability, intent, or history of actual or planned attack against United States assets.

Security Incident

A security compromise, infraction, or violation.

Security in-Depth

A determination made by the CSA that a contractor's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility.

Security Infraction

A security incident that is not in the best interest of security and does not involve the loss, compromise, or suspected compromise of classified information.

Security Level

A clearance or classification and a set of designators of special access approvals; i.e., a clearance and a set of designators of special access approval or a classification and a set of such designators, the former applying to a user, the latter applying, for example, to a computer object.

Security Officer

When used alone, includes both Contractor Program Security Officers and activity security officers at government facilities.

Security Policy

The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. A complete security policy will necessarily address many concerns beyond the scope of computers and communications.

Security Policy Automation Network

A wide area computer network sponsored by the Office of the Under Secretary of Defense (Policy Support) consisting of a Department of Defense-wide SECRET classified network and a separately supported unclassified network that supports communications with foreign among Department of Defense activities on foreign disclosure, export control, and international arms control and cooperation.

Security Policy Board

The Board established by the President to consider, coordinate, and recommend policy directives for United States security policies, procedures, and practices.

Security Profile

The approved aggregate of hardware/ software and administrative controls used to protect the system.

Security / Suitability Investigations Index

The Office of Personnel Management database for personnel security investigations.

Security Testing

A process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed application environment. This process includes hands-on functional testing, penetration testing, and verification.

Security Violation

Failure to comply with the policy and procedures established by the NISPOM that reasonably could result in the loss or compromise of classified information.

Self-Inspection

The internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this order and the implementing directives.

Senior Agency Official

The official designated by the agency head to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

Senior Foreign Official

Any foreign government official who, by virtue of position or access, may directly affect the government's policy. These officials include,

but are not limited to: those of ministerial rank and above; the heads of national departments, agencies and services; and representatives of ambassadorial rank and above.

Senior Intelligence Officer

The highest-ranking military or civilian individual directly charged with foreign intelligence missions, functions, or responsibilities within a department agency component, command, or element of an Intelligence Community organization.

Senior Officials of the Intelligence Community

The heads of organizations or activities within the Intelligence Community, as defined by the National Security Act of 1947, as amended, 50 United States Code 401a(4), and Executive Order 12333.

Senior Review Group

Provides the principle support to the SAPOC. The SRG is a “working level” group that reviews all SAPs prior to the Special Access Program Oversight Committee briefing.

Sensitive Activities

Sensitive activities are special access or Codeword programs, critical research and development efforts, operations or intelligence activities, special plans, special activities, or sensitive support to the customer or customer contractors or clients.

Sensitive But Unclassified Information

A term commonly and inappropriately used within the Department of Defense as a synonym for Sensitive Information. This is the preferred term.

Sensitive Compartmented Information

SCI is classified intelligence information concerning or derived from sensitive sources, methods or analytical processes which is required to be handled exclusively within formal access control systems established by Director of National Intelligence (DNI).

Sensitive Compartmented Information Courier – (Certified)

Sensitive Compartmented Information approved active duty military personnel, United States Government civilian employees, or contractor employees whose primary responsibility is to transport Sensitive Compartmented Information material worldwide. The individual is so designated in writing, and must have Sensitive Compartmented Information access approvals at the level of material being transported.

Sensitive Compartmented Information Courier – (Designated)

Sensitive Compartmented Information approved active duty military personnel, United States Government civilian employees, or contractor employees or consultants whose temporary responsibility is to transport Sensitive Compartmented Information material. The individual is so designated in writing, and must have Sensitive Compartmented Information access approvals at the level of material being transported.

Sensitive Compartmented Information Facility

Sensitive Compartmented Information Facility is an area, room, group of rooms, or installation accredited by the proper authority to store, use, host discussions of, and/or process Sensitive Compartmented Information (SCI).

Sensitive Compartmented Information Facility - Accreditation

Formal acceptance of a Sensitive Compartmented Information Facility as meeting Director of National Intelligence security standards and formal authorization to process, store, and/or discuss Sensitive Compartmented Information.

Sensitive Compartmented Information Facility – Co-utilization

The mutual agreement among two or more Government organizations to share the same Sensitive Compartmented Information Facility.

Sensitive Compartmented Information Facility Database

The Intelligence Community database that provides a single source listing of Sensitive Compartmented Information Facilities worldwide and is used to promote continuity of operations and relocation of affected resources in the event of a national emergency.

Sensitive Compartmented Information Facility – Fixed Facility Checklist

A standardized document used in the process of certifying a Sensitive Compartmented Information Facility. It documents all physical, technical, and

procedural security information for the purpose of obtaining an initial or subsequent accreditation. Such information shall include, but not be limited to: floor plans, diagrams, drawings, photographs, details of electrical, communications, heating, ventilation and air conditioning

Sensitive Information Computer Security Act of 1987

The Computer Security Law of 1987, Public Law No. 100-235 (H.R. 145), (Jan. 8, 1988), was passed by the United States Congress. It was passed to improve the security and privacy of sensitive information in Federal computer systems and to establish a minimum acceptable security practices for such systems. It requires the creation of computer security plans and the appropriate training of system users or owners where the systems house sensitive information.

It has been superseded by the Federal Information Security Management Act of 2002.

Sensitivity Label

A collection of information that represents the security level of an object and that describes the sensitivity of the data in the object. A sensitivity label consists of a sensitivity level (classification and compartments) and other required security markings (e.g., Codewords, handling caveats) to be used for labeling data.

Sensitive Position

Any position so designated within the Department of Defense, the occupant of which could bring

about, by virtue of the nature of the position, a materially adverse effect on the national security. All civilian positions are critical-sensitive, noncritical-sensitive, or non-sensitive.

Service

Honorable active duty (including attendance at the military academies), membership in ROTC Scholarship Program, Army and Air Force National Guard, Military Reserve Force (including active status and ready reserve), civilian employment in Government service, or civilian employment with a Department of Defense contractor or as a consultant involving access under the Department of Defense Industrial Security Program. Continuity of service is maintained with change from one status to another as long as there is no single break in service greater than 12 months.

Shipper

One who releases custody of material to a carrier for transportation to a consignee (See "Consignor.")

Signal Flags

The Intelligence Community database containing information used to assist security and counterintelligence professionals conducting National Agency Checks on individuals applying for positions with Intelligence Community organizations.

Significant Derogatory Information

Information that could justify an unfavorable administrative action, or prompt an adjudicator to Seek additional investigation or clarification.

Single Scope Background Investigation

The only Personnel Security Investigation conducted by Defense Security Service for the Department of Defense Personnel Security Program for TOP SECRET and Sensitive Compartmented Information duties. The period of investigation for a Single Scope Background Investigation is variable, ranging from three years for neighborhood checks to 10 years for local agency checks.

Single Scope Background Investigation – Periodic Reinvestigation

A periodic personnel security reinvestigation consisting for Top Secret clearances and/or critical sensitive or special sensitive positions consisting of the elements prescribed in Standard C of Intelligence Community Policy Guidance 704.1, "Investigative Standards for Background Investigations for Access to Classified Information." Initiated at any time following the completion of, but not later than five years, from the date of the previous investigation or reinvestigation.

Site Information Assurance Manager

The single Information systems security focal point for a defined site. The site Information Assurance Manager supports two organizations: User organization and technical organization. The Site

Information Assurance Manager is responsible for managing the baseline and ensuring that changes to the site baseline are properly controlled.

Site Security Manager (Construction)

A United States citizen, at least 18 years of age, cleared at the Top Secret level and approved for Sensitive Compartmented Information, responsible for security where a Sensitive Compartmented Information Facility is under construction.

Sole Proprietorship

A business owned by one individual who is liable for the debts and other liabilities incurred in the operation of the business.

Sound Group

Voice transmission attenuation groups established to satisfy acoustical requirements. Ratings measured in sound transmission class may be found in the Architectural Graphic Standards.

Sound Masking System

An electronic system used to create background noise to mask conversations and counter audio-surveillance threats.

Sound Transmission Class

The rating used in architectural considerations of sound transmission loss such as those involving walls, ceilings, and/or floors.

Source Document

A classified document, other than a classification guide, from which information is extracted for inclusion in another document.

Special Access Program

Any program that is established to control access, distribution, and to provide protection for particularly sensitive classified information beyond that normally required for TOP SECRET, SECRET, or CONFIDENTIAL information. A Special Access Program can be created or continued only as authorized by a senior agency official delegated such authority pursuant to Executive Order 13526, "Classified National Security Information".

Special Access Program Facility

A specific physical space that has been formally accredited in writing by the cognizant Program Security Officer which satisfies the criteria for generating, safeguarding, handling, discussing, and storing CLASSIFIED and/or UNCLASSIFIED Program information, hardware, and materials.

Special Access Programs Central Office

The primary DoD liaison with agencies of the Executive Branch and the Congress on all issues relating to DoD SAPs, except as noted in Reference (k). The Director, DoD SAPCO, shall be a flag officer or Senior Executive Service equivalent appointed by the Deputy Secretary of Defense.

Special Access Programs Coordination Office

The Department of Defense focal point for issues pertaining to Department of Defense controlled special access programs.

Special Access Program/Special Access Required

Any program imposing “need-to-know” or access control beyond those normally provided for access to Confidential, Secret, or Top Secret information. Such a program includes, but is not limited to, special clearance, adjudication, or investigative requirements; special designation of officials authorized to determine “need-to-know”; or special lists of persons determined to have a “need-to-know”.

Special Access Required Programs Oversight Committee

The senior Air Force Review Committee for overseeing resource allocation, acquisition, management, security, and execution of Air Force Special Access Programs (Excluding National Foreign Intelligence Program). The Secretary of the Air Force approves a Charter which describes the organization, composition, and functions of the Special Programs Oversight Committee.

Special Activity

An activity, or functions in support of such activity, conducted in support of national foreign policy objectives abroad that is planned and executed so that the role of the U.S. Government is neither apparent nor acknowledged publicly; but that is not intended to influence U.S., political processes,

public opinion, policies, or media, and does not include diplomatic activities or the collection and production of intelligence or related support functions.

Special Background Investigation

A personnel security investigation consisting of all the components of a Background Investigation plus certain additional investigative requirements. The period of investigation for a Special Background Investigation is the last 15 years or since the 18th birthday, whichever is shorter, provided that the last 2 full years are covered and that no investigation will be conducted prior to an individual's 16th birthday.

Special Investigative Inquiry

A supplemental personnel security investigation of limited scope conducted to prove or disprove relevant allegations that have arisen concerning a person upon whom a personnel security determination has been previously made and who, at the time of the allegation, holds a security clearance or otherwise occupies a position that requires a personnel security determination.

Special Program Document Control Center

The component's activity assigned responsibility by the Information System Security Representative for the management, control, and accounting of all documents and magnetic media received or generated as a result of the special program activity.

Special Program Review Group

The committee responsible for developing the Air Force Special Access Required programs resource requirements, including the Program Objective Memorandum, Budget Estimate Submission, and the President's Budget.

Special Security Center

The Director of National Intelligence element responsible for developing, coordinating, and overseeing Director of National Intelligence security policies and databases to support Intelligence Community security elements. The Special Security Center interacts with other Intelligence Community security organizations to ensure that Director of National Intelligence equities are considered in the development of national level security policies and procedures.

Sponsoring Agency

A government department or agency that has granted access to classified national intelligence, including Sensitive Compartmented Information, to a person whom it does not directly employ, e.g., a member of another government organization or a contractor employee.

Standard Practice Procedures

A document(s) prepared by a contractor who implements the applicable requirements of the DoD 5220.22-M, NISPOM, for the contractor's operations and involvement with classified information at the contractor's facility.

Standalone System

An Information systems operating independent of any other Information systems within an environment physically secured commensurate with the highest classification of material processed or stored thereon.

Stand-Alone Automated Information System

A stand-alone Automated Information System may include desktop, laptop, and notebook personal computers, and any other hand-held electronic device containing classified information. Stand-alone Automated Information systems by definition are not connected to any Local Area Network or other type of network.

Statement of Reasons

A letter from a Central Adjudication Facility to a subject, Notifying of the Central Adjudication Facility's intent to deny/revoke security clearance/eligibility, and the reasons for the proposed action.

Subcontract

Any contract entered into by a contractor to furnish supplies or services for performance of a prime contract or subcontract. For purposes of Department of Defense 5220.22-M (NISPOM) a subcontract is any contract, subcontract, purchase order, lease agreement, service agreement, request for quotation, request for proposal, invitation for bid (IFB), or other agreement or procurement action between contractors that requires or will require access to

classified information to fulfill the performance requirements of a prime contract.

Subcontractor

A supplier, distributor, vendor, or firm that furnishes supplies or services to or for a prime contractor or another subcontractor, who enters into a contract with a prime contractor. For purposes of Department of Defense 5220.22-M (NISPOM), each subcontractor shall be considered as a prime contractor in relation to its subcontractors.

Subject Matter Expert An expert in a particular field who contributes or verifies the accuracy of specific information needed by the project team.

Substantial Issue Information See: "Personnel Security- Issue Information"

Subsidiary

A corporation in which another corporation owns at least a majority of its voting securities.

Supporting Information Assurance Infrastructures

Collections of interrelated processes, systems, and networks that provide a continual flow of information assurance services throughout the Department of Defense, e.g., the key management infrastructure or the incident detection and response infrastructure.

Surreptitious Entry

Unauthorized entry in a manner which leaves no readily discernible evidence.

Survivability

The capability of a system to withstand a man-made or natural hostile environment without suffering an abortive impairment of its ability to accomplish its dedicated mission.

Suspicious Contact

Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee, all contacts by cleared employees with known or suspected intelligence officers from any country, or any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence services of another country.

System

Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. See also information system.

System Administrator

The individual responsible for maintaining the system in day-to-day operations. The System Administrator has responsibility to: manage system hardware and software, data storage devices and application software; manage system performance; provide system security and customer support; perform equipment custodian duties; maintain software licenses and documentation; monitor hardware and software maintenance contracts; establish Userid and

password; ensure adequate network connectivity; review audit trails; and provide backup of systems operations and other system unique requirements. See Information Assurance Officer

System Security Authorization Agreement

A formal document that fully describes the planned security tasks required to meet system or network security requirements. The package must contain all information necessary to allow the Designated Approving Authority to make an official management determination for authorization for a system, or site to operate in a particular security mode of operation; with a prescribed set of safeguards, against a defined threat with stated vulnerabilities and countermeasures; in a given operational environment; under a stated operational concept; with stated interconnections to external systems; and at an acceptable level of risk.

System Security Engineering

The efforts that help achieve maximum security and survivability of a system during its life cycle and interfacing with other program elements to ensure security functions are effectively integrated into the total system engineering effort.

System Security Plan

The formal document prepared by the IS owner (or common security controls owner for inherited controls) that provides an overview of the security requirements for the system and describes the

security controls in place or planned for meeting those requirements. The plan can also contain as supporting appendices or as references, other key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan. If two or more similar IS are to be operated in equivalent operational environments (e.g., the levels of concern and PL are the same, the users have at least the required clearances and access approvals for all information on the IS, the IS configurations are essentially the same, and the physical security requirements are similar), a Master SSP ((M)SSP) may be written by the ISSO, certified by the ISSM, and then approved by the CSA to cover all such IS. See *Master System Security Plan*.

System Software

Computer programs that control, monitor, or facilitate use of the Information System; for example, operating systems, programming languages, communication, input-output control, sorts, security packages and other utility-type programs. Considered to also include off-the-shelf application packages obtained from manufacturers and commercial vendors, such as for word processing, spreadsheets, data base management, graphics, and computer-aided design.

Systematic Declassification Review

The review for declassification of classified information contained in records that have been determined by the Archivist to have permanent historical value in accordance with title 44, United States Code.

Tactical Approval to Operate

Cognizant Security Authority delegated authority to an operational element to allow a Tactical Sensitive Compartmented Information Facility to be functional before formal accreditation is received. Tactical Approval to Operate may not exceed one year in duration.

Tactical Sensitive Compartmented Information Facility

An area, room, group of rooms, building, or installation accredited for Sensitive Compartmented Information –level processing, storage and discussion, that is used for operational exigencies (actual or simulated) for a specified period of time not exceeding one year.

Tactical Special Access Program Facility

An accredited area used for actual or simulated war operations for a specified period of time.

Target

An individual, operation, or activity which an adversary has determined possesses information that might prove useful in attaining his/her objective.

Tear Line

A place in an intelligence report (usually denoted by a series of dashes) at which the sanitized version of a more highly classified and/or controlled report begins. The sanitized information below the tear line should contain the substance of the information above the tear line, but without identifying the sensitive sources and methods. This

will permit wider dissemination, in accordance with the need-to-know, need-to-release, and write-to-release principles and foreign disclosure guidelines of the information below the tear line.

Technical Data

Information governed by “International Traffic in Arms Regulations” (ITAR) (Title 22, Code of Federal Regulations, Parts 120-130), and the Export Administration Regulation (EAR) (Title 15, Code of Federal Regulations, parts 368.1-399.2). The export of technical data that is inherently military in character is controlled by the ITAR. The export of technical data that has both military and civilian uses is controlled by the EAR.

Technical Security

A security discipline dedicated to detecting, neutralizing, and/or exploiting a wide variety of hostile and foreign penetration technologies. The discipline mandates training in various countermeasure techniques.

Technical Surveillance Countermeasures

Physical, electronic, and visual techniques used to detect and counter technical surveillance devices, technical security hazards, and related physical security deficiencies.

Technical Surveillance Countermeasures Surveys and Evaluations

A physical, electronic, and visual examination to detect technical surveillance devices, technical security hazards, and attempts at clandestine penetration.

Technical Surveillance Countermeasures Inspection

A government-sponsored comprehensive physical and electronic examination of an area by trained and specially equipped security personnel to detect or counter technical surveillance penetrations or hazards.

Technical Threat Analysis

A continual process of compiling and examining all available information concerning potential technical surveillance activities by intelligence collection groups which could target personnel, information, operations and resources.

Technical Vulnerability

A hardware, firmware, communication, or software weakness which leaves an Information System. open for potential exploitation or damage, either externally resulting in risk for the owner, user, or manager of the Information System.

Technology

The information and know-how (whether in tangible form, such as models, prototypes, drawings, sketches, diagrams, blueprints, or manuals, or in intangible form, such as training or technical services) that can be used to design, produce, manufacture, utilize, or reconstruct goods, including computer software and technical data, but not the goods themselves, or the technical information and know-how that can be used to design, produce, manufacture, use, or reconstruct goods, including technical data and

computer software. The term does not include the goods themselves.

Technology Control Plan

The document that identifies and describes sensitive program information; the risks involved in foreign access to the information; the participation in the program or foreign sales of the resulting system; and the development of access controls and protective measures as necessary to protect the U.S. technological or operational advantage represented by the system.

Technology Critical

Also referred to as militarily critical technology. Technologies that would make a significant contribution to the military potential of any country or combination of countries and that may prove detrimental to the security of the United States, consisting of:

- arrays of design and manufacturing know-how (including technical data);
- keystone manufacturing, inspection, and test equipment;
- keystone materials; and
- goods accompanied by sophisticated operation, application, or maintenance know-how.

Technology Transfer

Transferring, exporting, or disclosing defense articles, defense service, or defense technical data covered by the United States Munitions List to

any foreign person or entity in the United States or abroad.

Telecommunications

Preparation, transmission, communication or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means.

Telecommunications and Automated Information systems Security

Superseded by Information systems Security.

Telemetry

The science and technology of automatic data measurement and transmission, as by wire or radio, from remote sources, such as space vehicles, to a receiving station for recording and analysis.

Telemetry Intelligence

Technical and intelligence information derived from intercept, processing, and analysis of foreign telemetry; a subcategory of foreign instrumentation signals intelligence.

Telework

Any arrangement in which an employee performs officially assigned duties at an alternative worksite on either a regular or recurring, or on an ad hoc, basis (not including while on official travel).

TEMPEST

Short name referring to investigation, study, and control of compromising emanations from

telecommunications and information systems equipment.

TEMPEST Approved

This term applies to equipment or systems which have been built and certified to meet Level I of National Security Telecommunications Information System Security Advisory Memorandum TEMPEST/1-92, Compromising Emanations Laboratory Test Requirements.

TEMPEST Zone

A defined area within a facility where equipment with appropriate TEMPEST characteristics (TEMPEST zone assignment) may be operated with emanating electromagnetic radiation beyond the controlled space boundary of the facility.

TEMPEST Zoned Equipment

Equipment that has been evaluated and assigned an equipment zone corresponding to the level in NSTISSAM TEMPEST/1-92. This equipment must be installed according to the NSTISSAM and HQ-Level specialized installation instructions.

Temporary Access Eligibility

Access based on the completion of minimum investigative requirements under exceptional circumstances where official functions must be performed prior to completion of the investigation and adjudication process. Temporary eligibility for access may be granted before the investigations are complete and favorably adjudicated. The Temporary eligibility will be valid until completion of the investigation and adjudication; however,

the agency granting it may revoke it at any time based on unfavorable information identified in the course of the investigation. (See Interim Security Clearance)

Temporary Help/Job Shopper

An individual employed by a cleared company whose services are retained by another cleared company or Government activity performing on Special Access Program contracts and providing required services (e.g. computer, engineering, administrative support etc...) under a classified contractual agreement. This individual will have access to Special Access Program material only at locations designated by the utilizing activity.

Temporary Records

Federal records approved for disposal, either immediately or after a specified retention period. Also called disposable records.

Terrorism

The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

Threat

The sum of the potential strengths, capabilities, and strategic objectives of any adversary that can limit or negate United States. mission accomplishment or reduce force, system, or equipment effectiveness.

Threat Analysis

An Operations Security process which examines an adversary's technical and operational capabilities, motivation, and intentions, designed to detect and exploit vulnerabilities.

Threat Assessment

An evaluation of the intelligence collection threat to a program activity, system, or operation.

Threat Monitoring

The analysis, assessment, and review of Information System audit trails and other data collected for the purpose of searching out system events that may constitute violations or attempted violations of data or system security.

Toluene

A colorless flammable aromatic liquid obtained from coal tar or petroleum and used in some fuels, dyes, and explosives. It is also used as a solvent/thinner for some gums, lacquers, and paints; also called xylene or methylbenzene. At least one permanent marker on the market still contains toluene (AD Marker by Chartpak). These markers tend to be strong smelling, and may damage Compact Disc / Digital Video Discs.

TOP SECRET

The classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

Toolbox

SEE Computer Security Toolbox.

Transferred Records

Records transferred to Agency storage facilities or a federal records center.

Transmission Security

The component of Communications Security that results from all measures designed to protect transmissions from interception and exploitation by means other than crypto analysis.

Transmission

The sending of information from one place to another by radio, microwave, laser, or other non-connective methods, as well as by cable, wire, or other connective medium. Transmission also includes movement involving the actual transfer of custody and responsibility for a document or other classified material from one authorized addressee to another.

Transportation Plan

A comprehensive plan covering the movement of classified material between participants of an international program or project.

Transshipping Activity

A government activity to which a carrier transfers custody of freight for reshipment by another carrier to the consignee.

Trapdoor

Operating system and applications that usually have safeguards to prevent unauthorized

personnel from accessing or modifying programs. During software development, however, these built-in security measures are usually bypassed. Programmers often create entry points into a program for debugging and/or insertion of new code at a later date. These entry points (trapdoors) are usually eliminated in the final stages of program development, but they are sometimes overlooked, accidentally or intentionally. A perfect example of a trapdoor was dramatized in the movie *War Games*, where the teen-age hackers enters the special password "Joshua" and gains unrestricted access to a mainframe computer in North American Aerospace Defense Command headquarters. Such a mechanism in a computer's operating system can grant an attacker unlimited and virtually undetectable access to any system resource after presenting a relatively trivial control sequence or password.

Trusted Computing Base

The totality of protection mechanisms with a computer system, including hardware firmware, and software, the combination of which is responsible for enforcing a security policy. NOTE: The ability of a Trusted Computing Base to enforce correctly a unified security policy depends on the correctness of the mechanisms within the Trusted Computing Base, the protection of those mechanisms to ensure their correctness, and the correct input of parameters related to the security policy.

Trojan Horse

A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security (for example, making a “blind copy” of a sensitive file for the creator of the Trojan horse).

Trusted Computer System

A system that employs sufficient hardware and software integrity measures to allow its use for processing sensitive or classified information.

Trusted Path

A mechanism by which a person at a terminal can communicate directly with the trusted computing base. This mechanism can only be activated by the person or the trusted computing base and cannot be imitated by untrusted software.

Two-Person Integrity

A provision that prohibits one person from working alone.

Type 1 Products

Classified or controlled cryptographic item endorsed by the National Security Agency for securing classified and sensitive United States government information, when appropriately keyed. The term refers only to products, and not to information, key, services, or controls. They are available to United States. Government users, their contractors, and federally sponsored non-United States. government activities subject to export

restrictions in accordance with International Traffic in Arms Regulation.

Type Accepted Telephone

Any telephone whose design and construction conforms to the design standards for Telephone Security Group approved telephone sets.

(Telephone Security Group Standard #3, #4, or #5).

Umbrella Special Access Program

An approved Department of Defense Special Access Program that contains compartments for specific projects within the overall program. While there is no formal requirement to obtain separate approval for each individual project under the umbrella Special Access Program, each project must be consistent with the Special Access Program Oversight Committee - approved scope of the umbrella Special Access Program. The nickname, program description, and accomplishments of each significant project will be reported in the annual Special Access Program report. (Note: An individual participant's access can be afforded across-the-board at the umbrella level or specific individual project access can be granted on a limited (i.e., non-umbrella) level).

Unacknowledged Special Access Program

The existence of the Special Access Program is protected as special access and the details, technologies, materials, techniques, etc., of the program are classified as dictated by their vulnerability to exploitation and the risk of compromise. Program funding is often unacknowledged, classified, or not directly linked to the program. The four Congressional Defense Committees normally have access to the program.

Unauthorized Disclosure

An event involving the exposure of information to entities not authorized access to the information.

Unauthorized Person

A person not authorized to have access to specific classified information in accordance with the requirements of the NISPOM.

Unclassified Controlled Nuclear Information

Unclassified Controlled Nuclear Information under jurisdiction of the Department of Energy includes unclassified facility design information, operational information concerning the production, processing or utilization of nuclear material for atomic energy defense programs, safeguards and security information, nuclear material, and declassified controlled nuclear weapon information once classified as Restricted Data.

Department of Defense Unclassified Controlled Nuclear Information is unclassified information on security measures (including security plans, procedures and equipment) for the physical protection of Department of Defense Special Nuclear Material, equipment, or facilities.

Information is designated Unclassified Controlled Nuclear Information only when it is determined that its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of Special Nuclear Material, equipment, or facilities.

Unclassified Internet Protocol Router Network

Non-Secure Internet Protocol Router Network is used to exchange sensitive but unclassified information between “internal” users as well as providing user’s access to the Internet. Non-Secure Internet Protocol Router Network is composed of Internet Protocol routers owned by the United States Department of Defense. It was created by the Defense Information systems Agency to supersede the earlier Military Network.

Unclassified Sensitive

For computer applications, this term refers to any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal program, or the privacy to which individuals are entitled under the section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under the criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (Computer Security Act of 1987, Public Law 100-235). Also See Sensitive but Unclassified Information

Undercover Operation

A phrase that is usually associated with the law enforcement community and which describes an operation that is so planned and executed as to conceal the identity of, or permit plausible denial by, the sponsor.

Unfavorable Administrative Action

Adverse action taken as the result of personnel security determinations and unfavorable personnel security determinations.

Unfavorable Personnel Security Determination

A denial or revocation of clearance for access to classified information; denial or revocation of access to classified information; denial or revocation of a Special Access authorization (including access to Sensitive Compartmented Information); non-appointment to or non-selection for appointment to a sensitive position; non-appointment to or non-selection for any other position requiring a trustworthiness; reassignment to a position of lesser sensitivity or to a non-sensitive position; and non-acceptance for or discharge for the Armed Forces when any of the foregoing actions are based on derogatory information of personnel security significance.

Unified Network

A Unified network is a connected collection of systems or networks that are accredited (1) under a single System Security Plan, (2) as a single entity, and (3) by a single Cognizant Security Authority. Such a network Can be as simple as a small standalone Local Area Network operating at Protection Level 1, following a single security policy, accredited as a single entity, and administered by a single Information System Security Officer. Conversely, it can be as complex as a collection of hundreds of Local Area Networks separated over a wide area but still

following a single security policy, accredited as a single Cognizant Security Authority. The perimeter of each network encompasses all its hardware, software, and attached devices. Its boundary extends to all of its users.

United States

The 50 states and the District of Columbia.

United States and its Territorial Areas

The 50 states, the District of Columbia, Puerto Rico, Guam, American Samoa, the Virgin Islands, Wake Island, Johnston Atoll, Kingman Reef, Palmyra Atoll, Baker Island, Howland Island, Jarvis Island, Midway Islands, Navassa Island, and Northern Mariana Islands.

United States Citizen (Native Born)

A person born in one of the 50 United States, Puerto Rico, Guam, American Samoa, Northern Mariana Islands, U.S. Virgin Islands; or Panama Canal Zone (if the father or mother (or both) was or is, a citizen of the United States).

United States National

A citizen of the United States or a person who, though not a citizen of the United States, owes permanent allegiance to the United States, e.g., a lawful permanent resident of the United States. Categories of persons born in and outside the United States or its possessions who may qualify as nationals of the United States are listed in 8 United States Code 1101(a) and 8 United States Code 1401; subsection (a) paragraphs (1) through (7). Legal counsel should be consulted when

doubt exists as to whether or not a person can qualify as a national of the United States. NOTE: A United States national shall not be treated as a foreign person except when acting as a foreign representative.

Unscheduled Records

Federal records whose final disposition has not been approved.

Upgrade

A determination that certain classified information, in the interest of national security, requires a higher degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such a higher degree.

User

Individual, or system process acting on behalf of an individual, authorized to access an IS.

User Identification

A unique symbol or character string that is used by an Information System to uniquely identify a specific user.

Vault

A room(s) used for the storing, handling, discussing, and/or processing of Special Access Program information and constructed to afford maximum protection against unauthorized entry.

Vendor

The manufacturer or sellers of the Automated Information System equipment and/or software used on the special program.

Violation

Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information; or, any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of Executive Order 13526 or its implementing directives; or, any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of Executive Order 13526.

Virus

A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk.

Voting Securities

Any securities that presently entitle the owner or holder thereof to vote for the election of directors of the issuer or, with respect to unincorporated entities, individuals exercising similar functions.

Volatile Memory Components

Memory components that do not retain data after removal of all electrical power sources and when reinserted into a similarly configured Automated Information System do not contain residual data.

Vulnerability

Weakness in an IS, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Vulnerability Analysis

A process which examines a friendly operation or activity from the point of view of an adversary, Seeking ways in which the adversary might determine critical information in time to disrupt or defeat the operation or activity.

Vulnerability Assessment

The results of vulnerability analysis expressed as a degree of probable exploitation by an adversary.

Waived Special Access Program

An unacknowledged Special Access Program to which access is extremely limited in accordance with the statutory authority of Section 119e of 10 United States Code (reference b). The unacknowledged Special Access Program protections also apply to Waived Special Access Programs. Only the Chairman and the Senior Minority member (and, by agreement, their Staff Directors) of the four Congressional Defense Committees normally have access to program material.

Waiver

An exemption from a specific requirement.

Weapons of Mass Destruction

Chemical, biological, radiological, and nuclear weapons.

Wide Area Network

An interconnected network comprised of two or more separately accredited systems and/or networks.

Working Paper(s)

A draft classified document, portion of a classified document and material accumulated or created while preparing a finished document.

Workstation

A high-performance, microprocessor-based platform that uses specialized software applicable to the work environment.

Worm

A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

Write Protect

A term used to indicate that there is a machine hardware capability which may be manually used to protect some storage media from accidental or unintentional overwrite by inhibiting the write capability of the system. (For example, write protection of magnetic tapes is accomplished by the physical removal of the "Write-ring" from the back of the tape. Write protection on three and one half inch floppy diskettes refers to the correct placement of the sliding tab to the open position which inhibits the hardware capability to perform a physical write to the diskette. Write protection includes using optical disks within Compact Disc read-only devices.)

Acronyms

AAA	Army Audit Agency Access Approval Authority
AA&E	Arms, Ammunition, and Explosives
AAR	After-Action Report
ABCS	Army Battle Command System
AC	Alternating Current
ACA	Access Control Authority
ACADA	Automatic Chemical Agent Detector Alarm
ACCF	Army Central Clearance Facility
ACCM	Alternative Compensatory Control Measure
ACDA	US Arms Control and Disarmament Agency
ACERT	Army Computer Emergency Response Team
ACES	Automated Continuing Evaluation System
ACO	Administrative Contracting Officer
ACSI	Assistant Chief of Staff for Intelligence (Army) (former acronym; for new, See DCISINT)
ACPG	Advanced Chemical Protective Garment
ACS	Assistant Chief of Staff
ADP	Automated Data Processing
ADPSO	Automated Data Processing Security Officer
ADPSSO	Automated Data Processing System Security Officer
ADR	Adjudicative Desk Reference

ADS	Automated Data System
AEA	Atomic Energy Act of 1954 as amended, 42 U.S.C. 2011
AECA	Arms Export Control Act, 22 U.S.C. 2751 et seq.
AF	Air Force or Department of the Air Force
AFB	Air Force Base
AFC	Agreement for Cooperation
AFCAF	Air Force Central Adjudication Facility
AFI	Air Force Instruction
AFMAN	Air Force Manual
AFOSF	Air Force Office of Security Forces
AFOSI	Air Force Office of Special Investigations
AFOSP	Air Force Office of Security Police
AFPD	Air Force Policy Directive
AFR	Air Force Regulation
AFSCO	Air Force Security Clearance Office
AG/SCM	Advisory Group/Security Countermeasures
AHC	Ad Hoc Committee
AHG	Ad Hoc Group
AIA	Air Intelligence Agency Army Intelligence Agency Aerospace Industries Association
AID	Agency for International Development
AIQC	Antiterrorism Instructor Qualification Course
AIS	Automated Information systems
AISS	Automated Information systems Security

AISSP	Automated Information systems Security Plan
ALASAT	Air-Launched Anti-Satellite Weapon
ALBM	Air-Launched Ballistic Missile
ALCM	Air-Launched Cruise Missile
ALMC	Army Logistics Management College
AM	Amplitude-Modulated
AMCIT	American Citizen
AMP	Amended Mines Protocol
AMRAAM	Advanced Medium-Range Air-to-Air Missile
ANACI	Access National Agency Check w/ Written Inquiries
AO	Area of Operations
AOA	Area of Application
AOA	Analysis of Alternatives
AOS	Active Overflight System
AP	Armor Piercing
APC	Armored Personnel Carrier
APL	Antipersonnel Landmine
APM	Antipersonnel Mine
AQ-SAP	Acquisition Special Access Program
AR	Army Regulation
ARM	Anti-Radiation Missile
ARTY	Artillery
ASAT	Anti-Satellite Weapon
ASATS	Army Special Access Tracking System
ASBM	Air-to-Surface Ballistic Missile
ASD	Assistant Secretary of Defense

ASD C3I	Assistant Secretary of Defense C3I
ASD (NII)/DoD CIO	Assistant Secretary of Defense for Networks and Information Integration / Department of Defense Chief Information Officer
ASEP	Army SAP Enterprise Portal
ASIS	American Society for Industrial Security
ASM	Air-to-Surface Missile
ASP	Ammunition Supply Point
ASP	Accredited Security Parameters
ASPO	Acquisition Systems Protection Office
ASPP	Acquisition System Protection Program
ASPWG	Acquisition Systems Protection Working Group
ASSIST	Automated Systems Security Incident Support Team
AT	Assessment/Assistance/ Advance Team Anti-Tamper
ATEA	Anti-Tamper Executive Agent
AT/FP	Antiterrorism/Force Protection
ATL	Assessment/Assistance/ Advance Team Leader
ATO	Approval to Operate
ATOMAL	NATO Marking for US/UK Atomic Information
ATTU	Atlantic to the Urals
AUB	Agency Use Block
AVLB	Armored Vehicle Launch Bridge
AWG	American Wire Gauge

BACTO	Biological Arms Control Treaty Office [U.S. Army]
BAT	Base Assistance Team
BCE	Baseline Cost Estimate
BDA	Bilateral Destruction Agreement
BDI	Ballistic Defense Initiative
BDS	Biological Detection System
BES	Budget Estimate Submission
BI	Background Investigation
BIC	Bilateral Implementation Commission [SORT]
BIDS	Biological Integrated Detection System
BINAS	Biosafety Information Network Advisory System
BIOS	Basic Input/Output System
BIPN	Background Investigation plus Current National Agency Check
BIPR	Periodic Reinvestigation of Background Investigation
BIR	Background Investigation Requested
BIS	Bureau of Industry and Security [DOC, formerly BXA]
BISS	Base and Installation Security System
BITN	Background Investigation (10 Year Scope)
BL	Biosafety Level
BL	Bill of Lading
BM	Ballistic Missile
BMD	Ballistic Missile Defense
BMDO	Ballistic Missile Defense Organization

BMLNA	Ballistic Missile Launch Notification Agreement
BMS	Balanced Magnetic Switch
BOG	Board of Governors [IAEA]
BPAC	Budget Program Activity Code
BPPBS	Biennial Planning, Programming, and Budgeting System
BSDS	Biological Standoff Detection System
BSL	Biological Safety Level
BT	Battle Tank
BTO	Barbed-Tape Obstacle
BTW	Biological and Toxin Weapons
BTWC	Biological and Toxin Weapons Convention
BW	Biological Warfare/Weapons
BWC	Biological Weapons Convention
BXA	Bureau of Export Administration, Department of Commerce
(C)	Confidential
C or E	Conversion or Elimination
C2W	Command and Control Warfare
C3	Command, Control, and Communications
C3I	Command, Control, Communications, and Intelligence
C4	Command, Control, Communications, and Computers
CAA	Controlled Access Area
C&A	Certification and Accreditation
CAB	Civil Aeronautics Board

CAEST	Conventional Armaments and Equipment Subject to the Treaty
CAF	Central Adjudication Facility
CAGE	Commercial and Government Entity
CAM	Chemical Agent Monitor
CAMDS	Chemical Agent Munitions Disposal System
CAMIN	Chemical Accountability Management and Information Network
CAO	Contract Administration Office
CAPDS	Chemical Agent Point Detection System
CARDS	Chemical Agent Remote Detection System
CAS	Chemical Abstracts Service
CAS	Collaborative Adjudicative Services
CB	Citizen's Band
CBD	Chemical Biological Defense
CBDE	Chemical and Biological Defense Equipment
CBDP	Chemical Biological Defense Program
CBI	Confidential Business Information
CBIPM	Confidential Business Information Protective Measure
CBM	Confidence-Building Measure
CBO	Congressional Budget Office
CBR	Chemical, Biological, and Radiological
CBRD	Chemical, Biological, and Radiological Defense
CBRNE	Chemical, Biological, Radiological, Nuclear, and High-Explosive

CBW	Chemical and Biological Warfare/Weapons
CC	Chain of Command
CCB	Community Counterterrorism Board
CCB	Configuration Control Board
CCD	Conference of the Committee on Disarmament
CCI	Controlled Cryptographic Item
CCIR	Commander's Critical Information Requirements
CCISCMO	Community Counterintelligence & Security Countermeasures Office
CCL	Commerce Control List
CCMS	Case Control Management System
CCT	Case Closing Transmittal
CCTV	Closed-Circuit Television
CCVS	Central Clearance Verification System
CCW	Convention on Conventional Weapons
CD	Conference on Disarmament
CDC	Cleared Defense Contractor
CDC	Centers for Disease Control and Prevention
CDF	Chemical Agent Disposal Facility
CDR	Commander
CDR	Critical Design Review
CD-R	Compact Disk-Read
CD-ROM	Compact-Disk, Read-Only Memory
CDSE	Center for Development of Security Excellence
CDTF	Chemical Defense Training Facility

CEP	Continuous Evaluation Program
CERT	Committee of Emergency Response Team
CERT	Computer Emergency Response Team
CFE	Conventional Armed Forces in Europe Treaty
CFIUS	Committee on Foreign Investment in the United States
CFR	Code of Federal Regulations
CG	Command Guidance
CI	Counterintelligence Critical Information Character Investigation
CIA	Central Intelligence Agency
CID	Criminal Investigation Division
CIDC	Criminal Investigation Division Command (Army)
CIFA	Counterintelligence Field Activity
CIK	Crypto-ignition Key
CINC	Command-in-Chief
CIO	Central Imagery Office Chief Information Officer
CIPA	Classified Information Procedures Act
CIRT	Computer Incident Response Team
CISARA	Counterintelligence, Security Countermeasures & Related Activities
CISO	Counterintelligence Support Officer
CISSM	Component Information System Security Manager

CISP	Counterintelligence Support Plan
CISSP	Certified Information systems Security Professional
CJCS	Chairman of the Joint Chiefs of Staff
CLAS	Classified By
CLL	Chief of Legislative Liaison
CM	Classification Management Configuration Management Countermeasure
CMB	Configuration Management Board
CMC	Commandant of the Marine Corps Command Master Chief (Navy)
CFI	Classified Military Information
CMS	Community Management Staff
CMTS	Compliance, Monitoring and Tracking System
CMU	Concrete-Masonry Unit
CNAC	National Agency Check plus Credit Check
CNCI	Child Care National Agency Check plus Written Inquires and Credit Check [CNACI in OPM Components]
CNO	Chief of Naval Operations/Computer Network Operations
CNSS	Committee on National Security Systems
CNWDI	Critical Nuclear Weapon Design Information
COCOM	Coordinating Committee
COD	Cooperative Opportunities Document

COMINT	Communications Intelligence
COMPUSEC	Computer Security
COMSEC	Communications Security
CONEX	Container Express
CONOPS	Concept of Operations
CONPLAN	Contingency Plan
CONUS	Continental United States
CO	Commanding Officer
COO	Chief Operating Officer
COI	Community Of Interest
COOP	Continuity of Operations Plan
COPS	Committee on Physical Security
COR	Central Office of Record
	Contracting Officer Representative
COSMIC	NATO TOP SECRET
COTR	Contracting Officer's Technical Representative
COTS	Commercial Off-the-Shelf
COTS	Committee on Technical Security
CP	Command Post
CPAF	Cost Plus Award Fee (contract)
CPFF	Cost Plus Fixed Fee (contract)
CPI	Critical Program Information
CPIF	Cost Plus Incentive Fee (contract)
CPM	Contractor Program Manager
CPO	Chemical Protection Over- Garment
CPP	Counter Proliferation Policy

C-PR	Confidential – Periodic Reinvestigation
CPSO	Contractor/Command Program Security Officer
CPU	Central Processing Unit
CPWG	Crime-Prevention Working Group
CQ	Charge of Quarters
CRG	Compliance Review Group
CRIMP	Crime Reduction Involving Many People
CRS	Congressional Research Service
CRT	Critical Research Technology
CRYPTO	Cryptography
CSA	Cognizant Security Authority Cognizant Security Agency
CSBM	Confidence and Security Building Measure
CSE	Center for Security Evaluation
CSISM	COMSEC Supplement to the Industrial Security Manual
CSO	Cognizant Security Office Court Security Officer
CSRL	Common Strategic Rotary Launcher
CSS	Constant Surveillance Service Central Security Service
CSSI	Case Summary Sheet Information
CSSM	Communications-Computer System Security Manager
CSSO	Contractor Special Security Officer
CSSR	Case Summary Sheet Recommendation

CSSWG	Contractor SAP/SAR Security Working Group
CT	Counter Terrorism
CT&E	Certification Test and Evaluation
CTA	Common Table of Allowance
CTB	Comprehensive Nuclear Test-Ban
CTBT	Comprehensive Nuclear Test-Ban Treaty
CTBTO	Comprehensive Nuclear Test-Ban Treaty Organization
CTC	Counterterrorist Center
CTF	Chemical Transfer Facility
CTR	Cooperative Threat Reduction Program
CTS	COSMIC TOP SECRET
CTSA	COSMIC TOP SECRET ATOMAL
CTTA	Certified TEMPEST Technical Authority
CUA	Co-Utilization Agreement
CUI	Controlled Unclassified Information
CUSR	Central United States Registry
CVA	Central Verification Activity
CVS	Contractor Verification System
CW	Chemical Warfare/Chemical Weapons/ Codeword
CWC	Chemical Weapons Convention
CWCIP	Chemical Weapons Challenge Inspection Process
CWDF	Chemical Weapons Destruction Facility
CW-IWG	Chemical Weapons Implementation Working Group
CWPF	Chemical Weapons Production Facility
CWSF	Chemical Weapons Storage Facility

DA	Department of the Army
DAA	Designated Approving Authority Designated Accrediting Authority
DAA Rep	Designated Accrediting/Approving / Authority Representative
DAB	Defense Acquisition Board
DAC	Discretionary Access Control
DAE	Defense Acquisition Executive
DAF	Department of the Air Force
DAIG	Department of the Army Inspector General
DARPA	Defense Advanced Research Projects Agency
DC	Direct Current
DC	District of Columbia
DCAA	Defense Contract Audit Agency
DCAS	Defense Contract Administration Service
DCFL	Defense Computer Forensics Lab
DCHC	Defense Counterintelligence and Human Intelligence Center
DCI	Director of Central Intelligence
DCI SSC	Director of Central Intelligence Special Security Center
DCID	Director of Central Intelligence Directive
DCII	Defense Clearance and Investigations Index
DCIS	Defense Criminal Investigation Service
DCL	Declassify
DCMA	Defense Contract Management Agency

DCMC	Defense Contract Management Command
DCPDS	Defense Civilian Personnel Data System
DCPMS	Defense Civilian Personnel Management System
DCR	Developed Character Reference
DCS	Defense Courier Service
DCS	Deputy Chief of Staff
DCSINT	Deputy Chief of Staff for Intelligence Army
DD	Defense Department
DDEP	Defense Data Exchange Program
DDL	Delegation of Disclosure Authority Letter
DDSP/G	Department of Defense Security Police/ Guard
DECL	Declassify
DEIDS	Defense Eligibility Information Database System
DEERS	Defense Enrollment Eligibility Reporting System
DEPSECDEF	Deputy Secretary of Defense
DERV	Derived From
DES	Data Encryption Standard
DF	Declared Facility
DFA	Detailed/Draft Facility Agreement
DFAR	Defense Federal Acquisition Regulations
DFAS	Defense Finance and Accounting Service
DG	Director-General
DGR	Designated Government Representative

DHS	Department of Homeland Security
	Defense HUMINT Service
DIA	Defense Intelligence Agency
DIAC	Defense Intelligence Analysis Center
DIACAP	Department of Defense Information Assurance Certification and Accreditation Process
DIAM	Defense Intelligence Agency Manual
DICOB	Defense Industrial Security Clearance Oversight Board
DII	Defense Information Infrastructure
DIRNSA	Director, National Security Agency
DIS	Defense Investigative Service
DISA	Defense Information systems Agency
DISCO	Defense Industrial Security Clearance Office
DISCR	Directorate, Industrial Security Clearance Review
DISP	Defense Industrial Security Program
DITSCAP	Defense InfoTech Security Certification & Accreditation Process
DLA	Defense Logistics Agency
DMF	Data Management Facility
DMNS	Data Management Notification System
DMS	Data Management System
DMS	Defense Messaging System
DNA	Defense Nuclear Agency (former acronym; for new, See DTRA)
DNG	Downgrade

DNI	Director of National Intelligence/Director of Naval Intelligence
DOB	Date of Birth
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDIIS	Department of Defense Intelligence Information System
DoD IG	Department of Defense, Inspector General
DoDPI	Department of Defense Polygraph Institute
DoDSI	Department of Defense Security Institute
DOE	Department of Energy
DOHA	Defense Office of Hearings and Appeals
DOIS	Director of Industrial Security
DOJ	Department of Justice
DON	Department of the Navy
DONCAF	Department of the Navy Central Adjudication Facility
DOS	Department of State Disk Operating System
DOT	Department of Transportation
DPA	Defense Production Act
DPEP	Defense Personnel Exchange Program
DPG	Defense Planning Guidance
DPRB	Defense Planning and Resources Board
DPRO	Defense Plant Representative Office

DPS	Diplomatic Pouch Service
DRB	Defense Resources Board
DRAM	Dynamic Random Access Memory
DRMO	Defense Reutilization Management Office
DS	Direct Support
DSA	Designated Security Authority
DSB	Defensive Security Brief
DSCA	Defense Security Cooperation Agency
DSEC	Director of Security Army
DSMC	Defense Systems Management College
DSN	Defense Switched Network formerly AUTOVON
DSS	Defense Security Service
DSSS	Defense Special Security System
DSSCS	Defense Special Security Communication System
DSS-PIC	DSS Personnel Investigations Center
DT&E	Development Test and Evaluation
DTG	Date Time Group
DTIC	Defense Technical Information Center
DTIRP	Defense Treaty Inspection Readiness Program
DTM	Data-Transmission Media
DTOC	Division Tactical Operations Center
DTRA	Defense Threat Reduction Agency
DTS	Defense Transportation Service
DTSA	Defense Technology Security Administration

DUSD SP	Deputy Under Secretary of Defense for Security Policy
DVD	Digital Video Disk
EA	Atomic Energy Act
EAA	Export Administration Act of 1979
EAP	Emergency Action Plan
EAR	Export Administration Regulations
EC	Executive Council
ECCM	Electronic Counter-Countermeasures
ECM	Electronic Countermeasures
EDM	Emergency-Destruct measures
EECS	Electronic Entry-Control System
EEFI	Essential Elements of Friendly Information
EEI	Essential Elements of Information
EEPROM	Electronically Erasable Programmable Read Only Memory
EIF	Entry/Entered-Into-Force
EIS-TAO	Enterprise Information systems – Technology Applications Office
EKMS	Electronic Key Management System
ELECTRO-OPTINT	Electrical Optical Intelligence
ELINT	Electronic Intelligence
ELSEC	Electronic Security
EMSEC	Emission Security
ENAC	Entrance National Agency Check
ENAL	Entrance National Agency Check plus Special Investigative Inquiry
ENTNAC	Entrance National Agency Check
EO	Executive Order

EOC	Emergency Operations Center
EOD	Explosive-Ordnance Disposal
EOR	Element of Resource
EP	Electronic Protection
EPA	Environmental Protection Agency
EPCI	Enhanced Proliferation Control Initiative
EPITS	Essential Program Information, Technologies and Systems
EPL	Evaluated Products List
EPSQ	Electronic Personnel Security Questionnaire
EPW	Enemy Prisoner of War
E-QUIP	Electronic Questionnaire for Investigations Processing
ERB	Engineering Review Board
ES	Executive Secretary
ESEP	Engineer and Scientist Exchange Program
ESS	Electronic Security System
ET	Escort Team
EU	European Union
FA	Facility Agreement
FAA	Federal Aviation Administration Foreign Assistance Act of 1961, as amended
FAD	Facility Access Determination
FAR	Federal Acquisition Regulation
FAX	Facsimile
FBI	Federal Bureau of Investigation

FBIS	Foreign Broadcast Information Service
FCC	Federal Communications Commission
FCG	Department of Defense Foreign Clearance Guide, Department of Defense 4500.54-G
FCIP	Foreign Counterintelligence Program
FCL	Facility Security Clearance
FCT	Foreign Comparative Test
FDO	Foreign Disclosure Officer
FDS	Facility Data Sheet
FEMA	Federal Emergency Management Agency
FEPRM	Flash Erasable Programmable Read Only Memory
FFC	Fixed Facility Checklist
FFP	Firm Fixed Price (Contract)
FFRDC	Federally Funded Research and Development Center
FGI	Foreign Government Information
FHB	Former Heavy Bomber
FIDS	Facility Intrusion Detection System
FIEPSS	Fixed Installation Exterior Perimeter Security System
FIPC	Federal Investigations Processing Center
FIS	Foreign Intelligence Services
FISD	Federal Investigative Services Division
FISINT	Foreign Instrumentation Signals Intelligence 7
FIT	Foreign Inspection Team

FIU	Field investigative unit
FM	Frequency-Modulated
FMCT	Fissile Material Cutoff Treaty
FMS	Foreign Military Sales
FN	Foreign National
FOA	Field Operating Agency
FOC	Full Operational Capability
FOCI	Foreign Ownership, Control or Influence
FOIA	Freedom of Information Act
FOIA/PA	Freedom of Information Act/Privacy Act
FORDTIS	Foreign Disclosure and Technical Information System
FOUO	For Official Use Only
FPI	Fixed Price Incentive (Contract)
FPIF	Fixed Price Incentive Firm (Contract)
FPM	Federal Personnel Manual
FRD	Formerly Restricted Data
FRS	Facility Review Subgroup [IAEA]
FSC	Forum for Security Cooperation
FSL	Fixed Structure for Launcher
FSO	Facility Security Officer
FSP	Facility Security Profile
FSTS	Federal Security Telephone Service
FSU	Former Soviet Union
FVS	Foreign Visits System
FWA	Fraud, Waste, and Abuse
FY	Fiscal Year
FYDP	Five Year Defense Plan

G	GAMMA
G&A	General and Administrative
G2	Assistant Chief of Staff, G2 Intelligence
G-2	Staff Intelligence Officer Army and Marines
GAO	General Accounting Office
GCCS	Global Command and Control System
GC/MS	Gas Chromatography/Mass Spectrometry
GCA	Government Contracting Activity
GCO	GAMMA Control Officer
GDIP	General Defense Intelligence Programs
GENSER	General Service
GFE	Government Furnished Equipment
GFP	Government Furnished/Furnished Property
GHz	Gigahertz
GIG	Global Information Grid
GLBM	Ground-Launched Ballistic Missile
GLCM	Ground-Launched Cruise Missile
GMT	Greenwich Mean Time
GOCO	Government-Owned, Contractor-Operated
GOTS	Government Off-The-Shelf
GOVIND	Government-Industry Restricted Information
GPM	Government Program Manager
GPS	Global Positioning System
GSA	General Services Administration
GSA	General Security Agreement

GSC	Government Security Committee
GSOIA	General Security of Information Agreement
GSOMIA	General Security of Military Information Agreement
GTA	Graphic Training Aid
H	OPCW Highly Protected
HAC	House Appropriations Committee
HAS	Hardened Aircraft Shelter
HASC	House Armed Services Committee
HB	Heavy Bomber
HCA	Host Country Agreement
HDBT	Hardened and Deeply Buried Target
HE	High Explosive
HEU	Highly Enriched Uranium
HN	Host Nation
HNSC	House National Security Committee
HOF	Home Office Facility
HOIS	Hostile Intelligence Services
HPSCI	House Permanent Select Committee on Intelligence
HQ	Headquarters
HQ AFOTEC	Headquarters, Air Force Operational Test and Evaluation Center
HQ USAF/XOF	Headquarters Air Force Security Forces
HRO	Human Resources Office
HSP	Host State Party
HSPD	Homeland Security Presidential Directive

HT	Host Team
HTL	Host Team Leader
HUMINT	Human Intelligence
HVSACO	Handle Via Special Access Channels Only
Hz	Hertz
IA	Information Assurance
IACSE	Interagency Advisory Committee on Security Equipment
IAEA	International Atomic Energy Agency
IAM	Information Assurance Manager, synonymous with ISSM
IAO	Information Assurance Officer, synonymous with ISSO
IAR	Information Assurance Representative
IAT	Installation Assistance Team
IATT	Interim Approval To Test
IATO	Interim Approval To Operate
IAVA	Information Assurance Vulnerability Alert
IAW	In Accordance With
IBI	Interview Oriented Background Investigation
IC	Intelligence Community
ICAM	Improved Chemical Agent Monitor
ICAO	International Civil Aviation Organization
ICBM	Intercontinental Ballistic Missile
ICC	Inspection Coordination Center
ICC	Interstate Commerce Commission
ICD	Intelligence Community Directive

ICD	Initial Capabilities Document
ICP	Initial Control Point
ICR	Inventory Change Report
ID	Identification
IDC	International Data Center
IDE	Intrusion Detection Equipment
IDS	Intrusion Detection System
IED	Improvised Explosive Device
IEID	International Exchange of Infrasonic Data
IERD	International Exchange of Radionuclide Data
IESD	International Exchange of Seismological Data
IG	Inspector General
IG DoD	Inspector General of the Department of Defense
IID	Improvised Incendiary Device
IIR	Intelligence Information Report
IIT	International Inspection Team
IIV	Interim Inventory Verification
IMA	Intelligence Materiel Activity Army
IMD	Intelligence Materiel Detachment
IMINT	Imagery Intelligence
IMS	International Monitoring System
IMSP	Information Management Support Plan
INA	Integrated Notifications Application
INF	Intermediate-Range Nuclear Forces Treaty

INFCIRC	Information Circular [IAEA]
INFOSEC	Information systems Security
INMARSAT	International Maritime Satellite
IN-SAP	Intelligence Special Access Program
INSCOM	US Army Intelligence and Security Command
INTAC	Individual Terrorism Awareness Course
Interior	Department of the Interior
IOC	Intelligence Operations Center Initial Operational Capability
IOI	Item of Inspection
IOSS	Interagency OPSEC Support Staff
IOT&E	Initial Operational Test and Evaluation
IPB	Intelligence Preparation of the Battlefield
IPDS	Improved [Chemical Agent] Point Detection System
IFE	Individual Protection Equipment
IPIV	Initial Physical Inventory Verification
IPO	International Pact Organization
IR	Infrared
IR&D	Independent Research and Development
IRAC	Internal review and audit compliance
IRBM	Intermediate-Range Ballistic Missile
IRM	Information resource management
IRP	Inspection Readiness Plan
IS	Information System
ISA	International Security Agreement

ISB	Industrial Security Bulletin
ISCAP	Interagency Security Classification Appeals Panel
ISCOM	Naval Investigative Service Command
ISD	Inspectable Space Determination
ISDN	Integrated Services Digital Network
ISFD	Industrial Security Facilities Database
ISL	Industrial Security Letter
ISM	Industrial Security Manual
ISOO	Information Security Oversight Office
ISP	Inspected State Party
ISPG	Intelligence Programs Support Group
ISR	Industrial Security Regulation
ISRP	Information systems Requirements Package
ISS	Information systems Security Inspection Support Staff
ISS	Integrated Safeguards Subgroup
ISSE	Information System Security Engineer, synonymous with SDSO
ISSM	Information systems Security Manager, synonymous with IAM
ISSO	Information systems Security Officer, synonymous with IAO
ISSP	Information systems Security Professional
ISSR	Information systems Security Representative, synonymous with IAO
ISWG	Industrial Security Working Group
IT	Information Technology Inspection Team

ITAB	Information Technology Acquisition Board
ITAC	Intelligence and Threat Analysis Center
ITAR	International Traffic in Arms Regulations
ITC	Interagency Training Center
IVP	International Visit Program
IWC	Inhumane Weapons Convention
IWG	Interagency Working Group
J2	Intelligence Directorate, Joint Command
JACADS	Johnston Atoll Chemical Agent Disposal System defunct
JACIG	Joint Arms Control Implementation Group
JAFAN	Joint Air Force -Army -Navy
JAG	Judge Advocate General
JAGMAN	Judge Advocate General Manual
JAMS	Joint Adjudications Management System
JANAP	Joint Army, Navy, Air Force Publication
JCAVS	Joint Clearance and Access Verification System
JCG	Joint Consultative Group
JCIC	Joint Compliance and Inspection Commission [START]
JCITA	Joint Counterintelligence Training Academy
JCS	Joint Chiefs of Staff
JMIC	Joint Military Intelligence College
JMITC	Joint Military Intelligence Training Center

JMIP	Joint Military Intelligence Programs
JPAS	Joint Personnel Adjudication System
JROC	Joint Requirements Oversight Council
JS	Joint Staff Joint Service
JSAIWG	Joint SCI Accreditation/Inspection Working Group
JSAT	Joint Security Assistance Training
JSCP	Joint Strategic Capabilities Plan
J-SIIDS	Joint Services Interior Intrusion Detection System
JSP	Joint Service Program
JTF	Joint Trial Flight
J-TIDS	Joint Tactical Information Distribution System
Justice	Department of Justice
JVE	Joint Verification Experiment
JWICS	Joint Worldwide Intelligence Communication System
kHz	Kilohertz
KMP	Key Management Personnel
KT	Kiloton
LAA	Limited Access Authorization
LAC	Local Agency Check
LAN	Local Area Network
LBI	Limited Background Investigation
LBIP	Limited Background Investigation plus Current National Agency Check
LBIX	Limited Background Investigation Expanded

LBNA	Land-Based Naval Air
LC	Launch Canister
LCA	Limited Controlled Area
LCR	Listed Character Reference
LE	Law Enforcement
LEA	Law Enforcement Agency
LED	Light-Emitting Diode
LEU	Low Enriched Uranium
LFC	Local Files Check
LIMDIS	Limited Dissemination Limited Distribution
LLC	Limited Liability Corporation
LN	Local Network
LOA	Letter of Offer and Acceptance
LOA	Letter of Agreement
LOC	Letter of Consent Level of Concern
LOD	Letter of Denial
LOI	Letter of Intent
LON	Letter of Notification
LOS	Line of Sight
LOTS	Logistics Over The Shore
LP	Listening Post
LPF	Launcher Production Facility
LRA	Local Reproduction Authorized
LRC	Local Records Check
LRCN	Local Records Checks plus Investigation Requested
LRF	Launcher Repair Facility

LRIP	Low Rate Initial Production
LRNA	Long-Range Nuclear Air- Launched [Cruise Missile]
LSF	Launcher Storage Facility
LSN	Local Seismic Network
LTBT	Limited Test-Ban Treaty
LTM	Long-Term Monitoring
LRU	Lowest Replaceable Unit
MAA	Mission Area Analysis
MAC	Mandatory Access Control Military Airlift Command
MACOM	Major Command
MAD	Mutual Assured Destruction
MAIS	Major Automated Information systems
MAJCOM	Major Joint Command
MANPADs	Man-Portable Air Defense Systems
MASINT	Measurement and Signature Intelligence
MBA	Material Balance Area
MBI	Minimum Background Investigation
MBIP	Minimum Background Investigation plus Current National Agency Check
MBIX	Minimum Background Investigation Expanded
MBF	Military Biological Facility
MBR	Material Balance Report
MBT	Main Battle Tank
MC	Mitigating Conditions
MC&A	Materials Control and Accounting/ Accountability

MCO	Marine Corps Order
MCL	Munitions Control List
MCTL	Militarily Critical Technologies List
MDA	Missile Defense Agency (Formerly BMDO)
MDA	Milestone Decision Authorities
MDAP	Major Defense Acquisition Program
MDEP	Management Decision Package
MDMP	Military Decision-Making Process
MEVA	Mission-Essential or Vulnerable Area
MF	Maintenance Facility
MFA	Model Facility Agreement
MFO	Multiple Facility Organization
MI	Military Intelligence
MILCON	Military Construction
MILDEP	Military Department
MIL-STD	Military Standard
MINATOM	Ministry of Atomic Energy [Russian Federation]
MIRV	Multiple Independently- Targetable Reentry Vehicle
MISWG	Multinational Industrial Security Working Group
MLRS	Multiple Launch Rocket System
MNS	Mission Need Statement
MO	Modus Operandi Magneto-Optical
MOA	Memorandum of Agreement
MOBDES	Mobilization Designee

MOS	Military Occupational Specialty
MOU	Memorandum of Understanding
MP	Military Police/Manipulation Proof
MPACS	Military Police Automated Control System
MR	Mandatory Review
MRBM	Medium-Range Ballistic Missile
MRI	Mutual Reciprocal Inspection
MRV	Multiple Reentry Vehicle
MSIC	Military and Space Intelligence Center
MSPB	Merit Systems Protection Board
MSS	Munitions Sampling System
MT	Megaton
MTCR	Missile Technology Control Regime
MTMC	Military Traffic Management Command
MUF	Material Unaccounted For
MWD	Military Working Dog
NA	National Authority
NAC	National Agency Check
NACB	National Agency Check plus Written Inquiries and Credit Check plus Background Investigation Requested
NACI	National Agency Check plus Written Inquiries
NACIC	National Counterintelligence Center
NACL	National Agency Check plus Special Investigative Inquiry
NACLC	National Agency Check with Local Agency Checks & Credit Check

NACP	National Agency Check plus 10 Years Service
NACS	National Authority Coordinating Staff
NACSIM	National COMSEC Information Memorandum
NACW	National Agency Check plus Written Inquiries and Credit Check
NACZ	National Agency Check plus Written Inquiries and Credit Check plus Special Investigative Inquiry
NAF	Non-appropriated Funds Naval Air Facility
NAFI	Non-Appropriated Fund Investigation
NAG/SCM	National Advisory Group/Security Countermeasures
NAIC	National Air Intelligence Center
NARA	National Archives and Records Administration
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NAVATAC	Navy Antiterrorism Analysis Center
NAVCIRT	Navy Computer Incident Response Team
Navy	Department of the Navy
NBC	Nuclear, Biological & Chemical
NC	NATO CONFIDENTIAL NO CONTRACT
NCA	NATO CONFIDENTIAL ATOMAL National Command Authority

NCAF	Department of Navy Central Adjudication Facility
NCIC	National Crime Information Center
NCIS	Naval Criminal Investigative Service
NCMS	National Classification Management Society
NCO	Non-Commissioned Officer
NCS	National Communications System National Cryptologic School
NCSC	National Computer Security Center
NDA	Non-disclosure Agreement Non-Destructive Assay
NDE	Non-Destructive Evaluation
NDP	National Disclosure Policy
NDP-1	National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations
NDPC	National Disclosure Policy Committee
NDS	Non-Disclosure Statement
Net	Network
NF	See NOFORN
NFIB	National Foreign Intelligence Board
NFIP	National Foreign Intelligence Program
NFX	Nuclear-Free Zone
NGA	National Geospatial Intelligence Agency (formerly NIMA)
NGIC	National Ground Intelligence Center
NGO	Non-Governmental Organization
NIAG	NATO Industrial Advisory Group

NID	National Interest Determination
NII	National Information Infrastructure
NIMA	National Imagery and Mapping Agency (currently NGA)
NIPRNET	Non-Secure/Unclassified Internet Protocol Router Network
NIS	Naval Investigative Service
NISC	Naval Investigative Service Command
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NISPOMSUP	National Industrial Security Program Operating Manual Supplement
NISPPAC	National Industrial Security Program Policy Advisory Committee
NIST	National Institute of Standards and Technology
NLC	National Agency Check plus Local Agency Check plus Credit Check
NLT	Not Later Than
NMD	National Missile Defense
NMI	No Middle Initial
NMN	No Middle Name
NMMSS	Nuclear Materials Management Safeguards System
NN	Nick Name
NNAC	National Agency Check plus Written Inquiries and Credit Check plus Current National Agency Check
NNAG	NATO Naval Armaments Group

NNPA	Nuclear Non-Proliferation Act of 1978
NPI	No Pertinent Information
NNPI	Naval Nuclear Propulsion Information
NNWS	Non-Nuclear Weapon State
NOAC	National Operational Security Advisory Committee
NOCONTRACT	Not Releasable to Contractors or Contractor Consultants (Obsolete Marking)
NOFORN	Not Releasable to Foreign Nationals No Foreign National
NPC	Nonproliferation Center
NPLO	NATO Production and Logistics Organization
NPRC	National Personnel Records Center
NPRDC	Naval Personnel Research and Development Center
NPSB	National Agency Check plus Partial Special Background Investigation
NPT	Nuclear Non-Proliferation Treaty
NR	NATO Restricted
NRC	Nuclear Regulatory Commission
NRO	National Reconnaissance Office
NRRC	Nuclear Risk Reduction Center
NS	NATO SECRET
NSA	National Security Agency NATO SECRET ATOMAL
NSA/CSS	National Security Agency/Central Security Service
NSC	National Security Council

NSCO	NATO SECRET Control Officer
NSD	National Security Directive
NSDD	National Security Decision Directive
NSDM	National Security Decision Memorandum
NSF	National Science Foundation
NSG	Nuclear Suppliers Group
NSI	National Security Information
NS-IWG	Nuclear Safeguards Implementation Working Group [IAEA]
NSM	Network Security Manager
NSO	Network Security Officer
NSTISSAM	National Security Telecommunications Information systems Security Advisory Memorandum
NSTISSC	National Security Telecommunication Information Systems Security Committee
NSTISSI	National Security Telecommunications Information systems Security Instruction
NSTL	National Security Threat List
NTI	National Trial Inspection
NTISSC	National Telecom & Info Systems Security Commission
NTISSI	National Telecom & Information systems Security Instruction
NTISSP	National Telecommunications and Information systems Security Policy
NTK	Need To Know
NTM	National Technical Means
NTS	Nevada Test Site
NTT	Nuclear Testing Treaties

NU	NATO UNCLASSIFIED
NVD	Night-Vision Device
NVRAM	Non-Volatile Random Access Memory
NWFZ	Nuclear-Weapon Free Zone
NWS	Nuclear-Weapon State
NWSS	Nuclear Weapon Storage Site
OA, EOP	Office of Administration, Executive Office of the President
OADR	Originating Agency's Determination Required
OASD	Office of the Assistant Secretary of Defense
OCA	Original Classification Authority
OCONUS	Outside the Continental United States
ODC	Office of Defense Cooperation
ODNI	Office of the Director of National Intelligence
ODTC	Office of Defense Trade Controls, Department of State
Oe	Oersted
OI	Operating Instruction
OIG	Office of the Inspector General, Department of Defense
OISI	Office of Industrial Security, International
OJCS	Organization of the Joint Chiefs of Staff
OMB	Office of Management and Budget
OMIM	Operational Manual for Infrasound Monitoring
OMOSI	Operational Manual for On-Site Inspections

OMRM	Operational Manual for Radionuclide Monitoring
OMSM	Operational Manual for Seismological Monitoring
ONDCP	Office of National Drug Control Policy
ONI	Office of Naval Intelligence
OODEP	Owners, Officers, Directors, Executive Personnel
OOV	Object of Verification
OPAC-ALC	On-line Payment and Collection – Agency Locator Code
OPCW	Organization for the Prohibition of Chemical Weapons
OPF	Official Personnel File
OPIC	Overseas Private Investment Corporation
OPLAN	Operations Plan
OPM	The U.S. Office of Personnel Management
OPM	Office of Personnel Management
OPM	Office of Personnel Management
OPORD	Operations Order
OPR	Office of Primary Responsibility
OPSEC	Operations Security
ORCON	Dissemination and Extraction of Information Controlled by Originator
ORD	Operational Requirements Document
O&S	Operations and Support
OS	Treaty on Open Skies
OSCC	Open Skies Consultative Commission

OSCE	Organization for Security and Cooperation in Europe
OS-SAP	Operations and Support Special Access Program
OSD	Office of the Secretary of Defense
OSI	Office of Special Investigations, Air Force
OSI	On-Site Inspection
OSMAPS	Open Skies Management and Planning System
OSPG	Overseas Security Policy Group
OSRA	Open Skies Refueling Aircraft
OSTP	Office of Science and Technology Policy
OTA	Office of Technical Assessment
OT&E	Operational Test and Evaluation
OUSD A&T	Office of the Under Secretary of Defense Acquisition & Technology
OVP	Office of the Vice President
PA	Privacy Act
PAA	Principal Accrediting Authority Principal Approving Authority
PAC	Personnel access ceiling
PAL	Permissive Action Link
PAR	Program Access Request
PAS	Protected Aircraft Shelter
PASCODE	Personnel Accounting System Code
PB	President's Budget
PBD	Program Budget Decision
PC	Peace Corps
PCL	Personnel Security Clearance

PCO	Procuring Contracting Officer
PCS	Permanent Change of Station
PCU	Premise Control Unit
PD	Probability of Detection
PDA	Personal Digital Assistant
PDD	Presidential Decision Directive
PDD	Personal Digital Diary
PDM	Program Decision Memorandum
PDR	Preliminary Design Review
PDS	Protected Distribution System
	Practice Dangerous to Security
PED	Portable Electronic Device
PEM	Program Element Monitor
PEO	Program Executive Officer
PEP	Personnel Exchange Program
PERSEC	Personnel Security
PERSEREC	Personnel Security Research and Evaluation Center
PFIAB	President's Foreign Intelligence Advisory Board
PHOTINT	Photographic Intelligence
PI	Police Intelligence
	Preliminary Inquiry
PID	Personnel Identification Data
PII	Personally Identifiable Information
PIL	Physical Inventory Listing
PIPS	Personnel Investigations Processing System
PINS	Portable Isotope Neutron Spectroscopy

PIR	passive infrared
PIV	Physical Inventory Verification/Personal Identity Verification
PKI	Public Key Infrastructure
PL	Protection Level
PLA	Plain Language Address
PLAN	Operation Plan
PM	Program Manager
PMO	Program Management Office
PMCS D	Project Manager for Chemical Stockpile Disposal
PMD	Program Management Directive
PMNSCM	Program Manager for Non-Stockpile Chemical Material
PMO	Provost Marshal Office
PNE	Peaceful Nuclear Explosion
PNET	Peaceful Nuclear Explosions Treaty
POB	Place of Birth
POC	Point of Contact
POE	Point of Entry/Exit
POL	petroleum, oil, and lubricants
POM	Program Objective Memorandum
PONEI	Treaty Protocol on Notifications and Exchange of Information [CFE]
POV	Privately Owned Vehicle
PPBERS	Planning, Programming and Budgeting Execution Review System
PPBS	Planning, Programming and Budgeting System

PPCM	Perimeter and Portal Continuous Monitoring
PPP	Program Protection Plan
PPPF	Permitted Schedule 1 Protective Purposes Facility
PPR	Phased Periodic Reinvestigation
PPRA	Plutonium Production Reactor Agreement
PR	Periodic Reinvestigation
PREPCOM	Preparatory Commission/Committee
PREPCON	Preparatory Conference
PRI	Periodic Reinvestigation (required a prior investigation)
PROM	Programmable Read Only Memory
PROPIN	Proprietary Information
PRP	Personnel Reliability Program
PRS	Periodic Reinvestigation – SECRET
PRSC	Periodic Reinvestigation – SECRET/ CONFIDENTIAL
PS	Physical Security
PSAB	Personnel Security Appeals Board
PSAP	Prospective Special Access Program
PSD	Protective Security Detail
PSD	Program Security Directive
PSE	Physical Security Equipment
PSEAG	Physical Security Equipment Action Group
PSF	Phosphorus, Sulfur, or Fluorine Discreet Organic Chemicals
PSG	Program security guide

PSI	Personnel Security Investigation Physical-Security Inspector Program Security Instruction Proliferation Security Initiative
PSM	Program security manager
PSO	Program Security Officer
PSP	Personnel Security Program
PSQ	Personnel Security Questionnaire
PSS	Protective Security Service Personnel Security Specialist
PSWG	Personnel Security Working Group
PTBT	Partial Test-Ban Treaty
PU	Plutonium
QA	Quality Assurance
QC	Quality Control
QNSP	Questionnaire for National Security Positions
R&D	Research and Development
RAC	Request Authority to Conclude an agreement
RAISE	Rapid Assessment Incomplete Security Evaluation
RAM	Random Access Memory
RAN	Request Authority to Negotiate an agreement
RCA	Riot Control Agent
RD	Restricted Data
RDA	Research, Development, and Acquisition

RD&E	Research, Development, and Engineering
RDE	Radiation Detection Equipment
RDT&E	Research, Development, Test and Evaluation
REL TO	Releasable To
REMBASS	Remotely Monitored Battlefield Sensor System
REVCON	Review Conference
RF	Radio Frequency
RFA	Report for Adjudication
RFI	Representative of a Foreign Interest Radio Frequency Interference
RFP	Request for Proposal
RFQ	Request for Quotation
RII	Relevant Information and Intelligence
RIS	Reporting Identification Symbol
RL	Rocket Launcher
RLVP	Residual Level Validation Period
RM	Risk Management
RNLTD	Report Not Later Than Date
ROI	Report of Investigation
ROM	Read Only Memory
RON	Report of National Agency Check
RPO	Responsible Program/Project Office
RRU	Research, Recertify, Upgrade
RSI	Reimbursable Suitability Investigation
RSN	Reason for Classification (electronic messages)

RSO	Requesting State Party Observer
RTP	Research & Technology Protection
RTSO	Remote Terminal Security Officer
RUC	Reporting Unit Code
RV	Reentry Vehicle
RVOSI	Reentry Vehicle On-Site Inspection
S	SECRET
S2	Intelligence Officer, US Army
S&T	Science and Technology
SA	System Administrator
SAA	Special Approval Authority
SAC	Senate Appropriations Committee
SACS	Security Access Control Systems
SA/LW	Small Arms/Light Weapons
SAES	Security Awareness and Education Subcommittee
SAEWG	Security Awareness and Education Working Group
SAF	Secretary of the Air Force
SALT	Strategic Arms Limitation Talks defunct
SAM	Surface-to-Air Missile
SAMM	Security Assistance Management Manual
SAO	Special Access Office
SAP	Special Access Program
SAPCAF	Special Access Program Central Adjudication Facility

SAPCO	Special Access Program Coordination Office (Department of Defense OSD SAPCO)
	Special Access Program Control Officer
	Special Access Program Central Office (Component SAPCO)
SAPF	Special Access Program Facility
SAPI	Special Access Program Information
SAPOC	Special Access Program Oversight Committee
SAPWG	Special Access Program Working Group
SAR	Special Access Required
SAR	Synthetic Aperture Radar
SASC	Senate Armed Services Committee
SAT	Site Assistance/Assessment Team
SAV	Site Assistance/Assessment Visit or Visit with Special Right of Access
SBA	Small Business Administration
SBI	Special Background Investigation
SBII	Special Background Investigation plus Current National Agency Check
SBIP	Special Background Investigation/Single Scope Background Investigation plus Current National Agency Check
SBIR	Single Scope Background Investigation Requested
SBPR	Periodic Reinvestigation of Special Background Investigation/Single Scope Background Investigation
OSBU	Sensitive But Unclassified
SCA	Security Control Agreement

SCAR	Special control and access required
SCBA	Self-Contained Breathing Apparatus
SCC	Standing Consultative Commission
SCE	Service Cryptologic Element
SCG	Security Classification Guide
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCIPCCOM	Sensitive Compartmented Information Policy Coordination Committee
SCM	Security Countermeasure
SCR	Suspicious Contact Report
SDD	Secure Data Device
SDD	System Development and Demonstration
SDI	Strategic Defense Initiative
SDIO	Strategic Defense Initiative Organization
SDR	System Design Review
SDSO	System Design Security Officer, synonymous with ISSE/
SEC	Securities and Exchange Commission
SECDEF	Secretary of Defense
SECNAV	Secretary of the Navy
SECNAV INST	Secretary of the Navy Instruction
SES	Senior Executive Service
SETA	Security Education, Training and Awareness

SF	Security Forces Standard Form Special Forces
SI	Special Intelligence
SIF	Special/Suitability Issue File
SICBM	Small Intercontinental Ballistic Missile
SIGINT	Signals Intelligence
SIGSEC	Signals Security
SII	Special Investigative Inquiry Suitability/Security Investigation Index
SIO	Senior Intelligence Officer
SIOP	Single Integrated Operations Plan
SIOP/ESI	Single Integrated Operational Plan/ Extremely Sensitive Information
SIPRNET	Secret Internet Protocol Router/Routing Network
SIR	Safeguards Implementation Report
SIRT	Security incident response team
SISR	Signals Intelligence Security Regulation
SJA	Staff Judge Advocate
SLBM	Sea-Launched/Submarine- Launched Ballistic Missile
SLCM	Sea-Launched Cruise Missile
SLV	Space Launch Vehicle
SME	Significant Military Equipment
SMO	Security Management Office
SNDV	Strategic Nuclear Delivery Vehicle
SNM	Special Nuclear Material
SOI	Security Officer Identifier

SOIC	Senior Official of the Intelligence Community
SO/LIC	Special Operations/Low-Intensity Conflict
SOF	Special Operations Forces
SOFA	Status of Forces Agreement
SOFAR	Sound Fixing and Ranging
SON	Statement of Need Submitting office Number
SOP	Standard/Standing Operating Procedures
SOR	Statement of Requirement Statement of Reasons
SORT	Strategic Offensive Reductions Treaty
SOW	Statement of Work
SP	Security Police State Party
SPA	Special Purpose Access
SPECAT	Special Category
SPF	Security Policy Forum
SPG	Security Procedures Guide
SPINTCOM	Special Intelligence Communications
SPO	System Program Office
SPOC	Special Access Required Programs Oversight Committee
SPP	Standard Practice Procedures
SPR	SECRET – Periodic Reinvestigation
SPRG	Special Programs Review Group
SPSCI	Senate Permanent Select Committee on Intelligence

SPSCIF	Semi-Permanent Sensitive Compartmented
SPT	Site Preparation Team
SRAM	Static Random Access Memory
SRBM	Short-Range Ballistic Missile
SRF	Strategic Rocket Forces
SRG	Senior Review Group
SRM	Solid Rocket Motor
SRO	Special Review Office
SRR	System Requirements Review
SRTM	Security Requirements Traceability Matrix
SSA	Special Security Agreement
SSAA	System Security Authorization Agreement
SSAN	Social Security Account Number
SSBI	Single Scope Background Investigation
SSBN	Nuclear-Powered Ballistic Missile
SSCI	Senate Select Committee on Intelligence
SSCO	Special Security Contract Officer
SSDC	Space and Strategic Defense Command
SSEM	System Security Engineering Management or Manager
SSI	Suspect-Site Inspection
SSII	Suitability and Security Investigations Index
SSM	Surface-to-Surface Missile
SSM	System Security Manager
SSMP	System Security Manager Plan

SSN	Social Security Number
SSO	Special Security Officer
SSP	System Security Plan
SSR	Special Security Representative
SSS	Selective Service System
	Signature Security Service
	Strengthened Safeguards System
	Security Support Structure
SSSF	Single Small-Scale Facility
SSSP	Site Safeguards and Security Plan
SST	Site Survey Team
STA	System Threat Assessment
STANO	Surveillance, Target Acquisition, and Night Observation
STAR	System Threat Assessment Report
ST&E	Security Test and Evaluation
START	Strategic Arms Reduction Treaty
State	Department of State
STC	Sound-Transmission Coefficient
STD	Standard
STE	Secure Telephone Equipment
STI	Safeguards, Transparency, and Irreversibility
STS	Safeguards Technology Subgroup
STU	Secure Telephone Unit
STU-III	Secure Telephone Unit III
SVC	Special Verification Commission [INF]
TA/CP	Technology Assessment and Control Plan

TAD	Temporary Duty Assignment
TAFMSD	Total Active Federal Military Service Date
TAO	Technology Applications Office
TASM	Tactical Air-to-Surface Missile
TASO	Terminal Area Security Officer
TB	Technical Bulletin
TBD	To Be Determined
TC	Team Chief
TCO	Termination Contracting Officer Treaty Compliance Officer Technology Control Officer
TCP	Technology Control Plan
TCS	Temporary Change of Station
TDP	Technical Data Package
TDS	Technical Development Strategy
TDY	Temporary Duty
T&E	Test and Evaluation
TEI	Technical Equipment Inspection
TEL	Transporter Erector Launcher
TEMP	Test and Evaluation Master Plan
TEMPEST	Transient Electromagnetic Pulse Emanation Standard
TF	Training Facility
THAAD	Theater High Altitude Air Defense
THREATCON	Threat Condition
TIA	Transparency in Armaments Agreement
TIARA	Tactical Intelligence and Related Activities
TID	Tamper Indicating Device

TIMS	Treaty Information Management System
TJAG	The Judge Advocate General
TL	Training Launcher
TLC	Training Launch Canister
TLE	Treaty-Limited Equipment
TLI	Treaty-Limited Item
TM	Technical Manual
TM	Treaty Manager
TMD	Theater Missile Defense
TMDE	Test, Measurement, and Diagnostic Equipment
TMO	Technology Management Office Treaty Management Office
TMOM	Training Model of a Missile
TNS	Telephone Notification System
TOC	Treaty Operations Center
TOPS	Transportable Operational Planning System
TP	Transportation Plan
TPC	Two-person Control
TPDC	Training and Professional Development Committee
TPI	Two-person Integrity
TPS	Transportation Protection Service
TRADOC	U.S. Army Training and Doctrine Command
	Treasury Department of the Treasury
TRQ	TEMPEST Requirements Questionnaire

TS	TOP SECRET Technical Secretariat
TSA	Transportation Security Administration
TSC	Triple-Standard Concertina
T-SCIF	Tactical Sensitive Compartmental Information Facility
TSCM	Technical Surveillance Countermeasures
TSCO	TOP SECRET Control Officer
TSEC	Telecommunications Security
TSWA	Temporary Secure Working Area
TT	Technology Transfer
TTBT	Threshold Test-Ban Treaty
TTCP	Technology Transfer Control Plan
TTRA	Technology Targeting Risk Assessment
U	Unclassified
UA	User Agency
UCMJ	Uniform Code of Military Justice
UCNI	Unclassified Controlled Nuclear Information
UDOC	Unscheduled Discrete Organic Chemical
UIC	Unit Identification Code
UK	United Kingdom
UL	Underwriter's Laboratory
UN	United Nations
UNGA	United Nations General Assembly
UNMOVIC	United Nations Monitoring, Verification and Inspection Commission [Iraq]
UNSC	United Nations Security Council

UNSCOM	United Nations Special Commission on Iraq
UNTIA	United Nations Transparency in Armaments
UPS	Uninterruptible Power Supply
US	United States
USA	United States Army
USACIDU	U.S. Army Criminal Investigation Command (formerly Division, the acronym did not change)
USACIDC	U.S. Army Criminal Investigation Division Command
USAF	United States Air Force
USAINSCOM	U.S. Army Intelligence and Security Command
USAMI	U.S. Army Military Intelligence
USASMDC	U.S. Army Space and Missile Defense Command
USC	United States Code
US-CERTUS	Computer Emergency Readiness Team
USCG	United States Coast Guard
USD(A&T)	Under Secretary of Defense (Acquisition and Technology)
USD(AT&L)	Under Secretary of Defense (Acquisition, Technology, and Logistics)
USD(I)	Under Secretary of Defense (Intelligence)
USD(P)	Under Secretary of Defense (Policy)
USDA	Department of Agriculture
USERID	User Identification
USG	United States Government

USMC	United States Marine Corps
USML	United States Munitions List, 22 CFR 121
USN	United States Navy
USNA	United States National Authority
USPS	United States Postal Service
USSAN	United States Security Authority (NATO)
USSID	United States Signals Intelligence Directive
USSS	United States Secret Service
USTR	Office of the United States Trade Representative
UXO	Unexploded Ordnance
VA	Department of Veterans Affairs
VA	vulnerability assessment
VAL	Visitor Authorization Letter
VAR	Visit Authorization Request
VCC	Verification Coordinating Committee
VCJCS	Vice Chairman of the Joint Chiefs of Staff
VD	Vienna Document
VEREX	Group of Verification Experts
VIP	Very Important Person
WAN	Wide Area Network
WHCA	White House Communications Agency
WHG	Western Group of Forces [Soviet]
WHO	World Health Organization
WHS	Washington Headquarters Service
WINPAC	Weapons, Intelligence, Nonproliferation, & Arms Control

WMD	Weapons of Mass Destruction
WNINTEL	Warning Notice-Intelligence Sources & Methods Involved (Obsolete Marking)
WNRC	Washington National Records Center
WORM	Write Once Read Many
WSA	Weapons Storage Area
XMP	X-ray and manipulation proof
XNAC	Expanded National Agency Check
YYY MM DD	Year Month Date
YYMMDD	Year Month Date

Center for Development of Security Excellence



Center for Development of Security Excellence

CDSE

Learn. Perform. Protect.