OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

(1)

INTELLIGENCE

MEMORANDUM FOR: SEE DISTRIBUTION

JUN 13 2013

SUBJECT: DoD Security Lexicon

The attached DoD Security Lexicon (TAB A) represents the Department's definitions for the Information, Personnel, Physical, Special Access, and Industrial Security Programs. The Security Directorate will continue to coordinate with the Office of the Director of National Intelligence to ensure this lexicon aligns with the Intelligence Community Standard 700-1, "Intelligence Community Standard: Glossary of Security Terms, Definitions, and Acronyms," and will update the DoD Security Lexicon periodically, as appropriate. My point of contact is (b)(6)

HM Higgins
Deputy Under Secretary of Defense
(Intelligence & Security)

Attachment:
As stated

DISTRIBUTION:
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

A

DoD Security Lexicon*

(Information, Personnel, Physical, Special Access, and Industrial Security Programs)

Acceptable Level of Risk	An authority's determination of the level of potential harm that is acceptable.
Access	The ability or opportunity to gain physical proximity to property, assets, or knowledge of Controlled or National Security Information (NSI).
Access Approval	***Synonym(s)***: Access Authorization
Access Authorization	Documented approval to gain Access to assets, or a particular category or Classification Level of information. ***Synonym(s)***: Access Approval
Access Control	The process of granting or denying specific requests to: obtain or use Controlled Information and related information processing services; or enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances). A function or a system that restricts access only to authorized persons. ***Related Term(s)***: Access Control System ***Synonym(s)***: Entry Control; Physical Access Control
Access Control List	A database or list of individuals who are authorized Access to controlled information, property, or areas. ***Synonym(s)***: Access Roster
Access Control Point	The location at which a secure area allows for Ingress or Egress by vehicles or pedestrians. ***Synonym(s)***: Entry Control Point

Access Control System (ACS)	A human, automated, or electronic system or procedure that controls the ability of people or vehicles to enter a protected area, by means of authentication and authorization at designated Access Control Points. ***Synonym(s)*:** Physical Access Control System; Entry Control System
Access Credential	A physical artifact issued by the Federal, State or local government that attests to one's right to credit or authority. The access credential contains and/or depicts characteristics, authorizations, and privileges for physical access and internal security controls.
Access National Agency Check and Inquiries (ANACI)	A Personnel Security Investigation (PSI) for Access to classified information combining a National Agency Check (NAC), credit check, and residence, education, employment, and reference inquiries.)
Access Roster	***Synonym(s)*:** Access Control List
Access Suspension	***Synonym(s)*:** Suspension of Access
Accessioned Records	Records of Permanent Historical Value in the legal custody of NARA. These Records may, however, contain Classified Information remaining under the control of one or more executive branch agencies and require review for continued classification.
Accountable SCI	SCI determined by a Cognizant Security Authority (CSA) to require a Document Accountability Number (DAN) to aid in the traceability, retrieval, and audit of material.
Accreditation	The formal Certification by the designated Accrediting Official (AO) that a Facility, designated area, or information system has met specified security standards for handling, processing, discussing, disseminating, or storing information of a specified type or classification.

Accrediting Official (AO)	The Head of an IC Element (HICE), or a senior official delegated in writing by the HICE, holding the authority to formally accredit, re-accredit, or de-accredit a SCI Facility (SCIF) for operation based on its compliance with uniform security requirements, and support of a documented mission need. Accrediting Officials may issue Waivers of uniform security requirements where warranted by mission need, and may also exempt a SCIF from reciprocal use by other IC elements, again for mission need. ***Synonym(s)***: Designated Accrediting Authority; Delegated Accrediting Authority
Acknowledged Special Access Program	A SAP whose existence is acknowledged but its specific details (e.g., technologies, materials, or techniques) are classified as specified in the applicable Security Classification Guide. ***Related Term(s)***: Special Access Program
Acquisition Special Access Program	A SAP established to protect sensitive research, development, testing, and evaluation, modification, and procurement activities. ***Related Term(s)***: Special Access Program
Actionable Information	Information that potentially justifies an Unfavorable Adjudicative Determination.
Adjudication	The evaluation of pertinent data from a Personnel Security Investigation (PSI), as well as any other available information that is relevant and reliable, to determine whether a Covered Individual is: (1) suitable for government employment; (2) eligible for Logical and Physical Access; (3) eligible for Access to Classified Information; (4) eligible to hold a Sensitive Position; or (5) fit to perform work for or on behalf of the government as a Contractor Employee. ***Synonym(s)***: Adjudicative Process
Adjudicative Process	***Synonym(s)***: Adjudication

Adjudicator	An HR specialist, physical security specialist or personnel security specialist who performs adjudications..
Adversary	Any individual, group, organization, or government that conducts, or has the intention and capability to conduct, activities detrimental to the U.S. Government or its Assets.
Adverse Action	An action taken as the result of a security Infraction, Violation, or an Unfavorable Personnel Security Determination.
Adverse Information	Any information that reflects negatively on the integrity, trustworthiness, or character of an individual that: (1) suggests his or her ability to Safeguard classified information or serve in a National Security Position may be impaired; (2) indicates that his or her employment may not protect the integrity or promote the efficiency of the service; (3) justifies a decision not to issue Credentials; or (4) justifies refusal to grant Access to a building or installation. The terms Adverse, Derogatory, and Issue Information are used interchangeably. Adjudicative guidelines permit weighing minor issue information differently than substantial issue information when it comes to applying conditions, deviations, waivers, or revocations. ***Synonym(s):*** Issue Information; Derogatory Information *Minor Adverse Information:* Information that meets a threshold of concern, but for which Adjudication determines that adequate mitigation, as provided by the adjudicative guidelines, exists. Minor Adverse Information does not provide the basis for a Waiver or Condition. *Significant Adverse Information:* Information discovered during a Personnel Security Investigation (PSI) for Eligibility, Suitability, or Credentials that raises a flag requiring the

expansion of the Investigation.

Affiliate — Any entity effectively owned or controlled by another entity.

Agent of a Foreign Power — (1) Any person other than a United States Person, who (a) acts in the U.S. as an officer or employee of a foreign power, or as a member of a foreign power; (b) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the U.S. contrary to the interests of the U.S., when the circumstances of such person's presence in the U.S. indicate that such person may engage in such activities in the U.S., or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; (c) engages in International Terrorism or activities in preparation therefore; (d) engages in the international proliferation of Weapons of Mass Destruction (WMD), or activities in preparation therefor; or (e) engages in the international proliferation of WMD, or activities in preparation therefor for or on behalf of a foreign power. (2) Any person who (a) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the U.S.; (b) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the U.S.; (c) knowingly engages in sabotage or International Terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power; (d) knowingly enters the U.S. under a false or fraudulent identity for or on behalf of a foreign power or, while in the U.S., knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or (e) knowingly aids or abets any person in the conduct of activities described in subparagraph

	(a), (b), or (d) or knowingly conspires with any person to engage in activities described in subparagraph (a), (b), or (c).
Alarmed Zone	The totality of area covered by a premise control unit and associated sensors.
Alien	***Synonym(s)***: Foreign National
Ammunition	A device charged with explosives, propellants, pyrotechnics, initiating composition, riot control agents, chemical herbicides, smoke and flame, for use in connection with defense or offense, including demolition. Excluded from this definition are devices charged with chemical agents defined in JCS Pub 1-02, and nuclear or biological materiel. Ammunition includes cartridges, projectiles, including missile rounds, grenades, mines, and pyrotechnics together with bullets, shot and their necessary primers, propellants, fuses, and detonators individually or having a unit of issue, container, or package weight of 100 pounds or less. Blank, inert training ammunition and rim fire ammunition are excluded.
Analytical Risk Management (ARM)	The process of selecting and implementing security Countermeasures to achieve an Acceptable Level of Risk at an acceptable cost. ARM is a structured yet flexible approach to understanding security posture and developing effective security Countermeasures and options considering cost/benefit that is a snapshot in time that provides an audit trail.
Annunciation	The act of a sound or display indicator announcing which sensor has detected a change in state.
Anti-Passback	The prevention of repeat Access through any entrance reader by use of the same Credential, regardless of the holder, without first exiting through an exit reader.
Antiterrorism (AT)	Defensive measures used to reduce the Vulnerability of individuals and property to

	terrorist acts, to include limited response and containment by local military and civilian forces. Antiterrorism measures are taken to detect, deter, defend, defeat, and mitigate acts of terror.
Antiterrorism Officer (ATO)	A military or civilian advisor responsible for managing an Antiterrorism program.
Antiterrorism Plan (AT Plan)	The specific measures taken to establish and maintain an Antiterrorism program.
Appeal	(1) In Personnel Security, a formal request for review of a Denial or Revocation of Eligibility under the provisions of Executive Order. (2) In Information Security, a written request citing The Freedom of Information Act (FOIA) or Executive Order for reconsideration of information previously withheld from Release. ***Related Term(s)***: Due Process
Applicant	A person other than an Employee who has received an authorized conditional offer of employment for a position that requires Access to classified National Security Information (NSI), employment in a Sensitive Position, or Credentials under HSPD-12 guidelines.
Apportioned Special Access Program (SAP)	A DoD SAP that is formally included in the Integrated Joint Special Technical Operations (IJISTO) process for DoD Combatant Command use during deliberate planning, crisis action response, and operational deployment. ***Related Term(s)***: Special Access Program
Asset	A distinguishable entity that provides a service or capability and merits protection. Assets are people, physical entities, or information located either within or outside the United States and employed, owned, or operated by domestic, foreign, public, or private sector organizations.

Authentication	A process that matches presented information to the established origin of that information.
Authorized Adjudicative Agency	A department or agency that (1) determines Eligibility for occupancy of Sensitive Positions and Access to Classified Information and special programs for Employees, Contractors, consultants, detailees, and others, if applicable; (2) grants, denies, or revokes Security Clearances; (3) and directs and reviews Personnel Security Investigations (PSIs), criminal reports, polygraph reports, medical evaluations, counterintelligence Investigations, and other reports, as required.
Authorized Holder	***Related Term(s)***: Access ***Synonym(s)***: Authorized Person
Authorized Investigative Agency	A department or agency designated by the Security Executive Agent (SecEA) to conduct Personnel Security Investigations (PSIs) of persons to ascertain whether such persons satisfy the criteria for obtaining or retaining: (1) Eligibility for Access to Classified Information; (2) Suitability to hold a Sensitive Positions; or (3) Credentials under the provisions of HSPD-12.
Authorized Person	A person who has a favorable determination of Eligibility for Access to Classified Information, has signed an approved Nondisclosure Agreement (NdA), and has a Need-To-Know. ***Synonym(s)***: Authorized Holder
Authorizing Official	***Synonym(s)***: Designated Approval Authority
Authorized User	A user who has been granted permission to access specified systems, facilities, or equipment.
Automated Records Checks (ARC)	A method for requesting, collecting, and validating electronically accessible and adjudicatively-relevant data using the most efficient and cost-effective technology and

	means available.
Automatic Declassification	The principle of Declassification of information based solely upon: (1) the occurrence of a specific date or event as determined by the Original Classification Authority (OCA); or (2) the expiration of a maximum time frame for duration of Classification established by Executive Order.
Automatic Declassification Reviewer Certification	Formal course, with a required minimum review standard, that is developed, maintained, and taught by each agency providing instruction on proper identification of exemptible information that retains its classification 25-years beyond the date of Document creation.
Auxiliary Security Force (ASF)	A local, non-deploying military asset derived from host and tenant commands. The ASF is used to augment the installation Provost Marshal Office (PMO) during increased threat conditions. The ASF may fall under the control of the provost marshal or an officer designated by the commanding officer.
Background Investigation (BI)	This term is no longer in use. ***Synonym(s)***: Personnel Security Investigation
Badge	A security Credential that validates the possessor's authorization for Access to a Controlled Area or provides positive identification of the Badge holder. ***Related Term(s)***: Credential ***Synonym(s)***: Security Badge
Banner Line	The marking at the top (header) and bottom (footer) of each page of a classified Document that specifies both the Level of Classification and the applicable Control Markings. ***Related term(s)***: Page Marking; Banner Marking
Banner Marking	The markings at the top (header) and bottom (footer) of each page of a classified Document

	that specifies both the highest Level of Classification of information contained within the Document and the most restrictive Control Markings applicable. ***Related term(s)***: : Banner Line
Base Boundary	A line that delineates the surface area of a base for the purpose of facilitating coordination and deconfliction of operations between adjacent units, formations, or areas.
Base Defense	The measures, both normal and emergency, required to nullify or reduce the effectiveness of enemy attacks or sabotage.
Biographic Information	Facts that assert or support the establishment of an individual's idientity. The identity of U.S. citizens is asserted by their social security number and given name. Other biographic information may include, but is not limited to, identifying marks such as tattoos, birthmarks, etc.
Biometric	A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all biometric examples. An authenticator produced from measurable qualities of a living person.
Biometrics Reader	An Access Control device that verifies identity by analyzing and confirming a pre-recorded human characteristics.
Break In Service	A continuous (not cumulative) absence from service or employment greater than two years.
Card Reader	A device that communicates with an integrated circuit chip embedded in a smart card either by radio frequency (RF) signaling or by physical contact.
Carrier Custodian	***Synonym(s)***: Courier
Carve-out	A DoD provision approved by the Secretary or Deputy Secretary of Defense that relieves

	the Defense Security Service of its National Industrial Security Program (NISP) obligation to perform industrial security oversight functions for a DoD SAP. ***Related Term(s)*:** Special Access Program
Caveat	A distribution, warning, or admonishment statement applied to Classified or Controlled Unclassified Information to limit the dissemination or to provide additional safeguarding direction.
Central Adjudication Facility (CAF)	A centralized organization, authorized by DNI and agency head to evaluate reports of investigations (ROIs) and other relevant information and issue Eligibility determinations for Positions of National Security, Public Trust, Fitness, Suitability, or HSPD-12 Credentialing positions.
Central Alarm Monitoring System (CAM system)	A system consisting of electronically activated intrusion devices at a Facility or residence which, when activated, alerts a central alarm monitoring location. This central location may be a dispatcher who is able to direct a mobile react guard unit to the scene, or it may be an alerting device in the mobile react guard unit itself.
Certification	Comprehensive evaluation of the technical and non-technical security features and other Safeguards, made as part of and in support of the Accreditation process, to establish the extent that a particular design and implementation meet a specified set of security requirements.
Certification (Polygraph Examiner)	A formal and structured process to ensure that polygraph examiners and DoD PCASS examiners meet and maintain all necessary qualifications; receive the required formal instruction, training, and mentorship; and demonstrate technical proficiency to conduct examinations pursuant to standards established by The National Center for Credibility Assessment.

Certified TEMPEST Technical Authority (CTTA)	A U.S. Government Employee who has met established Certification requirements in accordance with the Committee on National Security Systems (CNSS) approved criteria and has been appointed by a U.S. Government department or agency to fulfill Certified TEMPEST Technical Authority (CTTA) responsibilities.
Chart (Polygraph)	The electronic display or analog recording of physiological data collected during a Polygraph Examination that is analyzed in the assessment of an individual's truthfulness.
Classification	The act or process by which information is determined to be Classified Information. ***Related Term(s)***: Classification Level
Classification and Control Markings Register and Manual (CAPCO Register)	The IC listing that identifies the official Classification and Control Markings, and their authorized abbreviations and Portion Markings used for all dissemination of classified national intelligence information. The Controlled Access Program Coordination Office (CAPCO) of the DNI/Special Security Directorate (SSD) maintains this system of classifications and controls.
Classification Authority Block	The classifier and Declassification instructions required for classified National Security Information (NSI); the block is placed at the bottom of a Document's first or title page and includes the following information: "Classified by"; "Reason" for Classification (used by OCAs) or "Derived From" (used by derivative classifiers); Declassification instructions and, when appropriate, Downgrading Instructions.
Classification Guide	A documentary form of classification guidance issued by an Original Classification Authority (OCA) that identifies the elements of information regarding a specific subject that have been determined to be classified and establishes the level and duration of

	Classification for each such element. ***Synonym(s)*:** Security Classification Guide
Classification Level	A category to which National Security Information (NSI) and material is assigned that denotes the degree of damage that Unauthorized Disclosure would cause to national defense or foreign relations of the United States, and the degree of protection required. There are three such levels: *Confidential, Secret,* and *Top Secret*. *Confidential (C)*: The Classification Level applied to information, the Unauthorized Disclosure of which reasonably could be expected to cause damage to the National Security. *Secret (S)*: The Classification Level applied to information, the Unauthorized Disclosure of which reasonably could be expected to cause serious damage to the National Security. *Top Secret (TS)*: The Classification Level applied to information, the Unauthorized Disclosure of which reasonably could be expected to cause exceptionally grave damage to the National Security.
Classification Management	The life-cycle management of classified Information from Original Classification to Declassification.

Classified Contract	Any contract requiring Access to Classified Information by a Contractor or Employees in the performance of the contract. (A contract may be a classified contract even though the contract document is not classified.) The security requirements prescribed are also applicable to all phases of pre-contract activity, including solicitations (bids, quotations, and proposals), pre-contract negotiations, post-contract activity, or other government contracting authority (GCA) program or project which requires Access to Classified Information by a Contractor.
Classified Information	Information that has been determined pursuant to Executive Order or the Atomic Energy Act of 1954 to require protection against Unauthorized Disclosure and is marked to indicate its Classified status when in documentary form. ***Related Term(s)***: National Security Information; Classification Level
Clear Zone	An area on both sides of a perimeter barrier that provides an unobstructed view of the barrier and the adjacent grounds.
Clearance	***Synonym(s)***: Personnel Security Clearance
Clearance Certification	An official notification that an individual holds a specific level of Security Clearance 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 (FCL) in accordance with the National Industrial Security Program (NISP).

Close and Continuing Contact	A relationship between two or more individuals, characterized by recurring, deliberate, mutual contact and continuing for a period of time, suggesting the relationship is more that than a casual acquaintance. ***Synonym(s)*:** Close and Continuing Relationship
Close and Continuing Relationship	***Synonym(s)*:** Close and Continuing Contact
Close Foreign Ties	Any recurring association or communication of any type with a Foreign National.
Closed Storage	The storage of information or equipment (including information systems) that is Classified, Sensitive, or Controlled Unclassified (CUI) in properly secured GSA-approved security containers and approved spaces, when the material is not in use and the space is not occupied by authorized personnel.
Closed Storage Area	A space constructed in accordance with established standards and authorized by the agency head or designee as meeting the requirements for secure storage of information or equipment (including information systems) that may be Classified, Sensitive, or Controlled Unclassified (CUI).
Coalition	An arrangement negotiated between one or more nations for: (1) common action; (2) multi-national action outside the bounds of established alliances, usually for single occasions or longer cooperation in a narrow sector of common interest; or (3) a force composed of military elements of nations that have formed a temporary alliance for some specific purpose.
Code Word	A single word assigned a Classification and a classified meaning to safeguard intentions and information regarding a classified plan, operation, or activity. ***Synonym(s)*:** Cryptonym

Cognizant Security Agency (CSA)	Agencies of the Executive Branch that have been authorized by Executive Order 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; DOE; CIA, as delegated by the DNI; and the NRC.
Cognizant Security Authority (CSA)	The person or official designated by the Head of a Department or Agency who serves as the responsible authority for all aspects of security program management concerning the protection of Classified Information or oversight for security requirements of those in Sensitive Positions. Synonym(s): Senior Security Authority
Cognizant Security Office (CSO)	The organizational entity delegated responsibility by the Head of a CSA to administer security programs on behalf of the CSA.
Cohabitant	A person with whom an applicant for or holder of a Security Clearance resides and shares bonds of affection, obligation, or other commitment, as opposed to sharing residence for reasons of convenience (e.g., a roommate). ***Related Term(s)***: Close and Continuing Contact
Collateral	Classified Information (i.e., Confidential, Secret, or Top Secret), which is not subject to enhanced security protection required for SAP information or SCI.
Collateral Area	A secure area or Vault accredited to process or store classified information at the Confidential, Secret, or Top Secret level.
Combating Terrorism (CbT)	All action taken to oppose terrorism throughout the entire threat spectrum, to include terrorist use of chemical, biological, radiological, nuclear materials, or high-yield

	explosive devices (CBRNE). Such actions include Antiterrorism (AT), Counterterrorism (CT), Terrorism Consequence Management, and intelligence support.
Commander	Military personnel specifically assigned to command positions within organizations.
Common Access Card (CAC)	The DoD Federal Personal Identify Verification (PIV) Card. ***Related Term(s)***: PIV Card
Communication Security (COMSEC)	The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications and to ensure the authenticity of such communications. COMSEC includes cryptosecurity, emission security, transmission security, and the Physical Security of COMSEC material and information.
Company	A generic and comprehensive term which may include sole proprietorships, individuals, partnerships, corporations, societies, associations, and organizations usually established and operating to carry out a commercial, industrial, or other legitimate business, enterprise, or undertaking.
Compartment	A category of protected information within an SCI or SAP Control System that requires a separate Access Control List (ACL) and Indoctrination. ***Related Term(s)***: Special Access Program
Compartmented Area (CA)	An area, room, or set of rooms within a SCI Facility (SCIF) that provides managed separation between Control Systems, Compartments, Sub-Compartments, or Controlled Access Programs.
Compartmented Intelligence	National Intelligence placed in a DNI-

	approved Control System to ensure handling by specifically identified and Access-approved individuals.
Compelling Need	A signed determination by the Head of an Intelligence Community Element (HICE), or designee, that the services, skills, or knowledge of an individual, based upon an assessment of risk, are deemed essential to operational or mission accomplishments.
Compensatory Measure	An alternate Physical Security Measure employed to provide a degree of security equivalent to that provided by a required Physical Security Measure or procedure. ***Related Term(s):*** Waiver; Exception
Competent Medical Authority	A licensed medical practitioner.
Competitive Service	All civilian positions in the Federal Government that are subject to 5 USC and are not specifically excepted from the civil service laws by statute, the President, or the OPM, and are not in the Senior Executive Service (SES).
Compilation	Information that is individually Unclassified or Classified at a lower level, but when aggregated or compiled in a single document, may become Classified or Classified at a higher level, if the aggregation reveals an additional association or relationship that meets the standards for Classified Information under an Executive Order. ***Synonym(s):*** Mosaic Effect
Compromise	The known or suspected exposure of Classified Information, clandestine activities, covert personnel, or sensitive Installations or Assets to an unauthorized person(s).
Compromising Emanations	Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by information system equipment. ***Related Term(s):*** TEMPEST

Condition	See Exception (Personnel Security).
Confidential (C)	See Classification Level.
Confidential Source	Any individual or organization that has provided, or that may reasonably be expected to provide, information to the U.S. on matters pertaining to the National Security with the expectation that the information or relationship, or both, are to be held in confidence.
Confidentiality	Assurance that information is not disclosed to individuals, devices, processes, or other entities lacking authorized Access.
Consequence	***Synonym(s)*:** Impact
Constant Surveillance	The use of human or technical resources to observe or protect a Facility by preventing unobserved Access and making known any unauthorized Access.
Construction Site Security Manager	A U.S. Citizen, at least 18 years of age, cleared at the Top Secret level and approved for SCI, responsible for security where a SCI Facility (SCIF) is under construction.
Construction Surveillance Technician (CST)	The person responsible to ensure the security integrity of a Facility while under construction who is: (1) a U.S. Citizen; (2) at least 18 years of age; (3) cleared at the Top Secret level; (4) experienced in construction; and (5) trained in accordance with established security standards.
Containerization	A box or other device in which a number of packages are stored, protected, and handled as a unit in transit; for example, CONEX, MILVAN, and SEAVAN. This term also refers to the shipping system based on large cargo-carrying containers that can be easily interchanged between trucks, trains, and ships, without re-handling of contents.
Continuity of Operations	The degree or state of being continuous in the conduct of functions, tasks, or duties

	necessary to accomplish a military action or mission in carrying out the National Military Strategy. It includes the functions and duties of the commander, as well as the supporting functions and duties performed by the staff and others acting under the authority and direction of the commander.
Continuous Evaluation	Review of the background and behavior of an individual who has been determined to be eligible for a Sensitive Position or for Access to Classified Information at any time during the period of Eligibility to determine whether that individual continues to meet those requirements. The review may include: (1) additional or new checks of commercial and government databases and other lawfully available information; (2) information provided under reporting requirements by the individual, supervisor, or coworker; (3) other relevant information systems audit data; or (4) an Expandable Focused Investigation (EFI).
Continuous Surveillance	Constant unobstructed observance of items or an area to prevent unauthorized Access, which may be maintained by dedicated guards, other on-duty personnel, or Intrusion Detection Systems (IDS) including those enhanced by closed-circuit television.
Contract Working Dog (CWD)	A Working Dog provided under contract and limited to performing defensive functions, and prohibited from offensive action or law enforcement evidentiary collection.
Contract Working Dog Team (CWDT)	A Working Dog and Handler provided under contract and subject to the same restrictions as a Contract Working Dog.

Contracting Officer (CO)	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 the designee's authority.
Contracting Officer's Representative (COR)	An individual, including a Contracting Officer's Technical Representative (COTR), designated and authorized in writing by the Contracting Officer to perform specific technical or administrative functions.
Contracting Officer's Technical Representative (COTR)	A certified Government Employee who is the business communications liaison between the U.S. Government and a Contractor. The COTR serves as the technical representative, and is responsible for authorizing specified actions and expenditures and for monitoring the day-to-day activities of the Contractor.
Contractor	(1) Any industrial, educational, commercial, or other entity that has executed a contract agreement with the Federal Government, a prime contractor or a foreign governmentand been granted a Facility Clearance (FCL) by a Cognizant Security Authority (CSA). (2) An individual (not appointed under 5 USC § 3109) providing expert, consultant, or personal services under contract, license, or other arrangement, either an employee of a Contractor entity, an independent personal services Contractor, a licensee, a certificate holder, a cooperative agreement participants, or grantee of any agency, including all Subcontractors. Contractor individuals, in order to perform the work specified under the contract, may require Access to space, information, information technology systems, staff, or Assets of the Federal Government.

Contractor Special Security Officer (CSSO)	A Contractor Employee formally designated by a company and approved by the Cognizant Security Authority (CSA) who is generally responsible for all aspects of SCI security management within the Contractor activity. ***Related Term(s)***: Special Security Officer
Control	The authority of the agency that originates information, or its successor in function, to regulate Access to the information. ***Related Term(s)***: Originator; Responsible Agency
Control Channel	***Synonym(s)***: Control System
Control Marking	Elements of the Banner Line and Portion Markings identifying special Control Systems that denote additional Access Control or physical protection for the information or items covered by the program (e.g., SCI) or identifying the expansion or limitation on the distribution of the information (i.e., Dissemination Control Markings). These markings are in addition to and separate from the Classification Level. ***Synonym(s)***: Marking
Control System	The system of procedural protective mechanisms used within SCI or SAP programs that provides the ability to exercise restraint, direction, or influence over, or provide that degree of Access Control or physical protection necessary to regulate, handle, or manage controlled information or items. ***Synonym(s)***: Control Channel
Controlled Access Approval	Authorization, coupled with a formal Indoctrination and signing of a Nondisclosure Agreement (NdA), for an individual to have Access to National Security Information within a Controlled Access Program, including SCI or SAP information.

Controlled Access Program	A DNI-approved program that protects three classes of National Intelligence programs: (1) *SCI* compartments; (2) IC *SAPs*; and (3) restricted Collateral information programs, other than SCI or SAPs, that impose 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. *SCI*: Classified national intelligence, concerning or derived from Intelligence Sources and Methods that must be protected within formal Control Systems established and overseen by the DNI. *IC SAP*:
Controlled Access Program Coordination Office (CAPCO)	An office responsible for providing two key services to the DNI and IC: oversight and management of all IC Controlled Access Programs and oversight and management of the IC's Classification and Control Markings system.
Controlled Area	An installation, facility, or space where access restrictions apply and that require physical security measures to safeguard personnel, property, or material. Unless measures are applied to qualify the area as a restricted area, controlled areas are not required to meet physical security standards to allow open storage of classified material or protection of high-value items. ***Synonym(s)***: Controlled Facility
Controlled Carrier Custodian	***Synonym(s)***: Courier
Controlled Cryptographic Item (CCI)	Secure telecommunications or information handling equipment and an associated cryptographic component that are Unclassified but governed by a special set of control requirements. Such items are marked "Controlled Cryptographic Item," or, where space is limited, "CCI."

Controlled Facility	***Synonym(s)***: Controlled Area
Controlled Unclassified Information (CUI)	Unclassified Information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies. ***Related Term(s)***: National Security Information, Classified Information
Controlling Organization	Agency, or its successor in function, that originates information or regulates Access to the information.
Corporate Family	The corporation, its subsidiaries, divisions, and branch offices.
Corroborate	Comparing information from any investigative source with that provided by the Subject of an investigation to confirm the information or to identify discrepancies.
Cost-Benefit Analysis	The comparison of costs and benefits relating to potential Countermeasures or mitigations and the selection of appropriate combinations designed to reduce Risk to an acceptable level within an acceptable cost.
Counter-Countermeasures (Polygraph) (Counter-CM)	Procedures invoked to defeat or confirm the presence of a suspected Countermeasure (CM).
Counterintelligence Scope Polygraph (CSP)	A screening Polygraph Examination that uses questions limited to prescribed counterintelligence (CI) issues.
Countermeasure (CM)	Any action, device, procedure, technique, or other measure taken to negate or mitigate an Adversary's ability to exploit Vulnerabilities.
Countermeasures (Polygraph) (CM)	Those strategies employed by examinees to affect polygraph testing by the intentional application of physical, mental, pharmacological, or behavioral tactics.

Counterterrorism (CT)	Offensive measures taken to prevent, deter, and respond to terrorism.
Country Clearance	The formal mechanism for U.S. Government Employees traveling on official business to seek permission to enter a country or visit the U.S. Mission to the United Nations.
Country Code	***Synonym(s)***: Trigraph
Courier	An individual with the appropriate Security Clearances who has been assigned responsibility for transporting shipments of classified materials. ***Synonym(s)***: Carrier Custodian; Controlled Carrier Custodian
Covered Individual	A person who performs or seeks to perform work for, or on behalf of, the Executive Branch, not including the President, the Vice President, or their respective Employees except as provided by 3 USC or annual appropriations acts.
Covered Position	A position (1) in the Competitive Service; (2) in the Excepted Service where the incumbent can be noncompetitively converted to the Competitive Service; and (3) in the Senior Executive Service (SES) by career appointment.
Credential	A physical artifact (such as a PIV card or a data object such as a digital certificate) issued by an authority for a lawful government purpose that attests to the possessor's right to Logical and Physical Access to classified information or material, or Controlled Facilities, Areas, or Information; or role as an official government representative in a law enforcement, investigative, security, or other designated function. ***Related Term(s)***: Badge
Credit Check	A review of information provided by credit bureaus or other sources pertaining to the credit history of the Subject of a Personnel

	Security Investigation (PSI).
Critical Asset	Any Facility, equipment, service, or resource considered essential to operations in peace, crisis, and war and warranting measures and precautions to ensure its continued efficient operation; protection from disruption, degradation, or destruction; and timely restoration.
Critical Information	Facts or details about friendly intentions, plans, capabilities, activities, operations, and missions that adversaries can effectively act upon and promote a Consequence detrimental to U.S. interests. ***Synonym(s):*** Essential Elements of Friendly Information
Critical Information List (CIL)	A consolidated list of a unit or organization's Critical Information.
Critical Infrastructure	Systems and Assets, whether physical or virtual, so vital to the U.S. that their incapacity or destruction would have a debilitating impact on Security, national economic security, national public health or safety, or any combination thereof.
Critical Infrastructure and Key Resources (CI/KR)	The combined range of civilian Assets deemed critical to the defense of the U.S. homeland whose loss would impose a debilitating effect on the Nation's security, economy, public health, safety, or government. ***Related Term(s):*** Critical Infrastructure; Key Resources
Critical Infrastructure Protection (CIP)	A multi-disciplinary security practice relating to the reduction of the overall Risk to Critical Infrastructure and Key Resources (CI/KR) Assets, systems, networks, functions, or their interconnecting links, that includes actions to deter the Threat, mitigate Vulnerabilities, or minimize the Consequences associated with a terrorist attack or other man-made or natural Hazard.

Critical Program Information (CPI)	Elements or components of a program for research, development, or acquisition that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability. CPI includes: (1) information about applications, capabilities, processes, and end-items; (2) elements or components critical to a military system or network mission effectiveness; or (3) technology that would reduce U.S. technological advantage if it came under foreign control.
Criticality Assessment	The deliberative process used to identify Assets needing protection by weighing, for each Asset, its importance, the effect of a terrorist attack, and the difficulty of post-attack recovery.
Critical-Sensitive Positions	Those positions within the following categories with the potential to cause exceptionally grave damage to the National Security. Such positions require: (1) Access to Top Secret or "Q" Classified Information; (2) development or approval of war plans, or plans or particulars of future major or special operations of war, or critical and extremely important items of war; (3) National Security policy-making or policy-determining; (4) investigative duties such as counterintelligence Investigations; (5) Adjudication, recommendation of adjudicative determinations, and/or granting of Personnel Security Clearances (PCLs); (6) duty on personnel security boards; or (7) the same degree of trust within the National Security community. ***Related Term(s)*:** Sensitive Position
Crypto-ignition key (CIK)	Device or electronic key that contains information used to electronically lock and

	unlock cryptoequipment.
Cryptonym	***Synonym(s)*:** Code Word
Current Investigation File	A report of investigation that has been conducted within the number of years specified by policy for a given purpose.
Custodian	An individual who has possession of, or is otherwise charged with, the responsibility for safeguarding property or Classified Information.
Damage Assessment	A formal multi-disciplinary analysis to determine the effect of a Compromise of Classified Information on the National Security.
Damage to the National Security	Harm to the national defense or foreign relations of the U.S. from the Unauthorized Disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.
Data Owner	***Synonym(s)*:** Responsible Agency
De-accreditation	The formal Certification by a Cognizant Security Authority (CSA) that a Facility, designated area, or information system has been determined to no longer be required for handling, processing, discussing, disseminating, or storing SCI and has been cleared of all SCI.
Debarment	A prohibition from taking a Competitive Service examination or from being hired or retained in a Covered Position for a specific time period. Or, when a contractor or its employees have been excluded or debarred from federal contracting on the System for Award Management (SAM) at www.sam.gov.
Debriefing	***Synonym(s)*:** Termination Security Briefing
Deception Indicated (Polygraph) (DI)	This term is no longer in use. ***Synonym(s)*:** Significant Response

	(Polygraph)
Declassification	The authorized change in the status of Classified Information to Unclassified Information.
Declassification Authority	The documented authority to declassify material. Those officials include: (1) the Originator, if still serving in the same position; (2) the Originator's current successor in function; (3) a supervisory official of either (1) or (2); or (4) an official with delegated Declassification Authority, in writing, by the agency head or the Senior Agency Official of the Originating Agency.
Declassification Exclusion	Information of Permanent Historical Value that is older than 25 years and marked as Restricted Data (RD) or Formerly Restricted Data (FRD), which excludes it from the Automatic Declassification because it is subject to the provisions of the Atomic Energy Act of 1954, as amended.
Declassification Guide	Written instructions issued by a Declassification Authority that describe the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.
Declassification Guide (Permanent Records)	Written instructions issued by a Declassification Authority that have been approved by the Information Security Classification Appeals Panel (ISCAP) and that include a detailed description of the information, an explanation about why the information should be exempted from Declassification and must remain classified for a longer period of time and a specific date or specific and independently verifiable event for Automatic Declassification of specific Records that contain the information.
Decompartmentation	The removal of information from a Compartment without altering the information to conceal sources, methods, or analytical

	procedures.
Defense Central Index of Investigations (DCII)	A centralized database, organized in a searchable format, of selected unique identifying information and Security Clearance data utilized by security and investigative agencies in the DoD, as well as selected other Federal agencies, to determine Security Clearance status and the existence or physical location of criminal and Personnel Security investigative files. The DCII database is physically maintained by the Defense Manpower Data Center; however, the data that it contains is the responsibility of the contributing agencies.
Defense Courier Service (DCS)	An organization that provides for the secure and expeditious transportation and delivery of qualified material that requires controlled handling by Courier. ***Related Term(s):*** Courier
Defense Security Enterprise (DSE)	The organizations, infrastructure, and measures (to include policies, processes, procedures, and products) in place to Safeguard DoD personnel, information, operations, resources, technologies, and Facilities against harm, loss, or hostile acts and influences. This comprises Personnel, Physical, Industrial, Information, Operations, chemical and biological, and SAP Security, as well as security training and research and technology protection, and aligns with Information Assurance, Foreign Disclosure and security cooperation, cybersecurity, nuclear physical security, and Antiterrorism policy.
Defense Security Executive (DSE)	The designee under USD(I) who has responsibility for policy development and oversight of the Defense Security Enterprise (DSE).
Defense Security Program	The programmatic planning, expenditures,

	and return on investment estimating process for the Defense Security Enterprise (DSE).
Defensive Security Briefing (DSB)	Formal advisories that alert traveling personnel to the potential for harassment, exploitation, provocation, capture, entrapment, or criminal activity.
Delay Time	The total time an intruder is prevented from gaining Access to a secured resource to include the penetration time provided by structural barriers, the Ingress Time to reach the secured resource, and the Egress Time to load the secured resource and exit the Facility. ***Related Term(s)***: Egress Time
Delegated Accrediting Authority	***Synonym(s)***: Accrediting Official
Denial	(1) In Personnel Security, an adjudicative decision based on a Personnel Security Investigation (PSI), other relevant information, or both, that a person is ineligible for Access to Classified Information. (2) In Information Security, a written statement to a Mandatory Declassification Review (MDR) requester disapproving a request for information, or portions of information, in accordance with the applicable Executive Order.
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 Level 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.
Derogatory Information	***Synonym(s)***: Adverse Information

Design Basis Threat (DBT)	The Threat against which an Asset must be protected and upon which the protective system's design is based. It is the baseline type and size of threat that buildings or other structures are designed to withstand, and the tactics aggressors will use against the asset, and the tools, weapons, and explosives employed in these tactics.
Designated Accrediting Authority	***Synonym(s)*:** Accrediting Official
Designated Approval Authority (DAA)	The official with the authority to formally assume responsibility for operating a system at an Acceptable Level of Risk. ***Synonym(s)*:** Authorizing Official
Designated Disclosure Authority (DDA)	A military or civilian government official commonly referred to as a Foreign Disclosure Officer (FDO), appointed by the head of an OSD organizational element or a DoD component or by their Principal Disclosure Authority (PDA), who has been delegated authority in a Delegation or Disclosure Authority Letter to control disclosures of classified military information (CMI) and Controlled Unclassified Information (CUI) to foreign governments and international organizations. The DDA must be an official of such grade and position that the person has Access to the appointing PDA or head of the OSD organizational element or DoD Component. ***Synonym(s)*:** Foreign Disclosure Officer
Designated Government Representative	An official with the requisite Security Clearance, who is designated in writing, and who (1) acts for the sending government to verify the existence of a valid export or disclosure authorization and to approve transfer arrangements for classified material; or (2) acts for the recipient government in receipting for and accepting security

	responsibility of the classified material on behalf of the recipient government.
Designated Intelligence Disclosure Officer (DIDO)	The designated senior authority within an IC element responsible for that element's Foreign Disclosure and Release decisions and whose name and position are certified to the DNI in writing and other U.S. officials designated by the DNI. This term in no longer in use. ***Synonym(s):*** Senior Foreign Disclosure Authority
Designated Security Authority	The senior government official responsible for establishing security policy and procedures for international programs.
Detectable Actions	Physical actions or entities and emissions or other phenomena that can be observed, imaged, or detected by human senses or by active and passive sensors.
Determination Authority	A designee of a Head of an Intelligence Community Element (HICE) with responsibility for decisions rendered with respect to SCI Eligibility or ineligibility. ***Synonym(s):*** SCI Access Determination Authority
Developed Reference	A source that the investigator learns of independently, through investigative field work, and whose identity was not made known by the Subject of the Investigation, either on the Personnel Security Questionnaire (PSQ), during the Personnel Security Investigation (PSI), or through a contact of the Subject.
Deviation	See Exception.
Digraph	A two-letter acronym for a classified Code Word or Nickname.
Digital Identity	The representation of an established identity in a digital environment. Identity authentication rquires that the digital identity be based off of, or verified

	against, the authoritative source of the respective identity attributes.
Director of Central Intelligence Directive (DCID)	A directive issued by the Director of Central Intelligence (DCI) prior to the formation of the Office of the Director of National Intelligence (ODNI) that establishes general policies and procedures to be followed by intelligence agencies and organizations that were under DCI jurisdiction prior to the passage of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). Note: IC Directives (ICDs), IC Policy Memoranda (ICPMs), and IC Policy Guidance (ICPG) issued by the DNI supersede DCI Directives.
Disclosure	The sharing of Unclassified or Classified Information, whether verbal, written, or by any other means, to an authorized recipient without providing a copy for retention
Dissemination Control Markings	Markings that identify the expansion or limitation on the distribution of information. ***Related Term(s)***: Control Marking
Distribution Statement	A statement used on a controlled Document to denote the extent of its availability for secondary distribution, Release, and Disclosure without additional approvals or authorizations. A Distribution Statement is distinct from and in addition to a security Classification Marking and any Dissemination Control Markings included in the Banner Line.
Document	***Synonym(s)***: Record
Document Accountability Number (DAN)	A number assigned to an accountable Document providing traceability, retrieval, and auditing capabilities.

Domestic Terrorism	Activities that (1) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; (2) appear to be intended (a) to intimidate or coerce a civilian population, (b) to influence the policy of a government by intimidation or coercion, or (c) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and (3) occur primarily within the territorial jurisdiction of the United States.
Downgrading	A determination by a Declassification Authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.
Dual Citizen	Any person who is simultaneously a citizen of more than one country.
Due Process	An established administrative process, designed to ensure fair and impartial adjudication of facts and circumstances, that is offered to individuals before a final Unfavorable Adjudicative Determination of: (1) Eligibility for Access to National Security Information (NSI); (2) Suitability or Fitness for employment for or on behalf of the U.S. Government; or (3) Eligibility for Physical or Logical Access. Due Process provides the individual with adequate notice of the basis for the unfavorable determination, a reasonable opportunity to be heard regarding the underlying facts and circumstances, and an opportunity to appeal.
Duress Alarm System	A method by which authorized personnel can covertly communicate a situation of duress to a security control center or to other personnel in a position to notify a security control center.
e-Application	A web-based tool for self-reporting biographic details, declarations, clarifications, and mitigating information necessary to conduct investigations.

Egress Time	The interval required for an intruder to load and carry stolen Assets from a secure area when theft is the purpose of the penetration. ***Related Term(s)***: Delay Time
Electronic Questionnaire for Investigations Processing (e-QIP)	A secure web-based automated system that facilitates timely, accurate processing of investigation requests to an Investigative Service Provider (ISP). Agencies authorize applicants to access the system to enter data and documents required for the investigation, and the system collects data from the Applicant based on the appropriate investigative questionnaire. ***Related Term(s)***: Personnel Security Questionnaire
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 non-electronic communication, without the consent 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 communications and the use of tagging, tracking, and location devices.
Eligibility	A formal determination that a person meets the Personnel Security requirements for Access to a specified type or types of classified information, occupancy of a Sensitive Position (Suitability), or Logical or Physical Access to Controlled Facilities under HSPD-12 provisions.
Emergency Action Plan (EAP)	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.

Emergency Communications Center (ECC)	The single emergency response dispatch point that has the ability to: (1) provide continuous, uninterrupted receipt and processing of emergency calls; (2) dispatch sufficient resources to mitigate the emergency; (3) provide the required follow-on communications related to the situation; and (4) meet public law.
Employee	(1) A person, other than the President and Vice President, employed by, detailed or assigned to, or acting for an agency, including members of the Armed Forces; (2) an expert or consultant to an agency; (3) an industrial or commercial Contractor, licensee, certificate holder, or grantee of an agency, including all Subcontractors; (4) a personal services contractor; or (5) any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head.
Employee Assistance Program (EAP)	A program sponsored by an agency designed to provide counseling and referral services to Employees having personal, alcohol, drug, financial, behavioral, or emotional problems.
Employment Reference	An individual with direct knowledge of a Subject's character and conduct in the workplace, such as a supervisor, coworker, or subordinate.
Encryption	Transforming data into an unintelligible form in order to conceal its meaning. Two typical cases are: (1) End-to-End encryption – encryption of information at the origin within a communications network, with decryption postponed to the final destination point; and (2) Link encryption – the application of on-line crypto operations to a link of communications system so that all information passing over the link is encrypted.

Enhanced Subject Interview (ESI)	An in-depth interview between a trained and certified investigator and the Subject of Investigation to develop a full understanding of the Subject's background as a required part of an Investigation and to offer the Subject an opportunity to explain, clarify, refute, or mitigate issues or discrepant information. The ESI shall explore the presence or absence of all potentially disqualifying conditions and mitigating factors.
Entrance National Agency Check (ENTNAC)	A Personnel Security Investigation (PSI) scoped and conducted in the same manner as a National Agency Check (NAC) except that an FBI technical fingerprint search is not conducted.
Entry Control	***Synonym(s)***: Access Control
Entry Control Point (ECP)	***Synonym(s)***: Access Control Point
Entry Control System (ECS)	***Synonym(s)***: Access Control System
Equity	Information (1) originally classified by or under the Control of an agency; (2) in the possession of the receiving agency in the event of transfer of function; or (3) in the possession of a successor agency for an agency that has ceased to exist. ***Related Term(s)***: Control
Equity Holder	***Synonym(s)***: Responsible Agency
Escort	Personnel trained and authorized to accompany visitors not authorized a permanent access Badge to the Facility; or a cleared individual who accompanies a shipment of classified material to its destination.
Escorted Individuals	Persons who require access, without a determination of fitness, who must be accompanied at all times by a sponsor with authorization to escort.

Espionage	Those activities designed to obtain, deliver, communicate, or transmit information relating to the national defense with the intent or reason to believe such information will be used to the injury of the U.S. or to the advantage of a foreign nation or transnational entity.
Essential Elements of Friendly Information (EEFI)	This term is no longer in use. ***Synonym(s)*:** Critical Information
Essential Elements of Information (EEI)	The most critical information requirements regarding the Adversary and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision.
Excepted Service	All positions in the Executive Branch of the Federal Government which are specifically excepted from the Competitive Service by or pursuant to statute, the President, or OPM, and which are not in the Senior Executive Service (SES).
Exception (Personnel Security)	An adjudicative decision to grant initial or continued Eligibility despite failure to meet the full adjudicative or investigative standards. There are three types of Exceptions: *Condition, Deviation,* and *Waiver.* *Condition*: 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. *Deviation*: Eligibility granted or continued despite either a Significant Gap in coverage or Scope in the Investigation or an out-of-date Investigation.

Waiver: The granting or continuance of Eligibility despite the presence of Significant Adverse Information that would normally preclude Access. The approval authority shall approve a Waiver only when the benefit of Access clearly outweighs any security concerns. Within the IC approval authorities are the DNI, Head of IC Element (HICE), or principal designee; within the DoD, the approval authority is the DoD Component head or designee. A Waiver may require prescribed limitations on Access such as additional security monitoring.

Exception (Physical Security)

An approved exclusion from a standard or requirement or continuation of a non-standard condition that creates a Vulnerability and requires Compensatory Measures. There are four types of Physical Security Exceptions: *Deviation, Limited Exception, Permanent Exception,* and *Waiver.*

Deviation: The inability to achieve a minimum Physical Security standard for Facilities, equipment, or procedures.

Limited Exception: An approved long term Deviation from minimum Physical Security standards due to a security condition that can be corrected within three years.

Permanent Exception: Approval of a permanent Deviation from minimum Physical Security standards.

Waiver: Approval of a short-term Deviation from minimum Physical Security standards due to a security condition that can be corrected within one year. Within the IC, see Waiver (Physical Security).

Exemption (Automatic Declassification)	Overriding of the otherwise Automatic Declassification of information of Permanent Historical Value when it is older than 25 years, exempted by Executive Order, and covered by an authorized Declassification Guide.
Expandable Focused Investigation (EFI)	Tailored investigative leads conducted to develop and resolve identified issues and explore the potential for other pertinent issues sufficient to make an informed decision when an eApplication, Investigation, or Continuous Evaluation flags potential issues.
Expanded Scope Polygraph	***Synonym(s)*:** Expanded-Scope Screening
Expanded-Scope Screening (ESS)	An examination that includes the questions from a Counterintelligence Scope Polygraph (CSP) and questions related to falsification of security forms, involvement with illegal drugs, and criminal activity. ***Synonym(s)*:** Full Scope Polygraph; Expanded Scope Polygraph
Explosives	A chemical compound mixture or device, the primary or common purpose of which is to function by explosion. The term includes, but is not limited to, individual landmines, demolition charges, and blocks of explosives (dynamite, trinitrotoluene, C-4, and other high explosives) consisting of 10 or more pounds.
Facility	Real property of a department, agency, or contractor within which classified or sensitive activities may be conducted.
Facility Certification	An official notification to the accreditor of the Physical, procedural and Technical Security acceptability of a Facility to protect Classified Information.
Facility Clearance	***Synonym(s)*:** Facility Security Clearance
Facility Security Clearance (FCL)	An administrative determination by the U.S. Government that, from a security viewpoint, a Company is eligible for Access to Classified

	Information of a certain category (and all lower categories). ***Related Term(s)***: Security Clearance ***Synonym(s)***: Facility Clearance
Facility Security Officer (FSO)	A Contractor Employee formally designated by a Company and approved by the Cognizant Security Authority (CSA) to assume certain security and administrative functions of a Collateral classified program or contract in accordance with National Industrial Security Program (NISP) guidelines. ***Related Term(s)***: Security Professional
Federal Records	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 U.S. 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 or exhibition purposes, extra copies of Documents preserved only for convenience of reference, and stocks of publications and of processed Documents are not included. ***Related Term(s)***: Record; Presidential Records
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 form, or have some other relationship arising

	out of their creation, receipt, or use, such as restrictions on Access or use. Also documentary material, regardless of its physical form or characteristics, that is arranged in accordance with a filing system or maintained as a unit because it pertains to the same subject, function, or activity.
File Series Exemption (FSE)	Written instructions issued by a Declassification Authority regarding a File Series that contain information that falls within one or more of the Exemption categories contained in an Executive Order and approved for use by the Information Security Classification Appeals Panel (ISCAP). The FSE only applies to Records within the specific File Series. The Records remain subject to Mandatory Declassification Review (MDR) requests.
Financial Disclosure Program (FDP)	The program that implements statutory and Executive Order requirements placed on all Employees in the Executive Branch who need regular Access to Particularly Sensitive Classified Information, as a condition of maintaining Access to such information, to submit relevant information concerning their financial condition, which also includes information regarding spouses and dependents. ***Related Term(s)*:** Particularly Sensitive Classified Information
Fitness	The level of character and conduct determined necessary for an individual to perform work for or on behalf of a Federal agency as an Employee in the Excepted Service (other than a position subject to Suitability) or as a Contractor. ***Related Term(s)*:** Suitability; Excepted Service; Contractor
Fitness Determination	A decision by an agency regarding an individual's Fitness that in and of itself does not obligate the agency to appoint or contract with an individual.

	Related Term(s): Excepted Service; Contractor
Fixed Facility Checklist (FFC)	A standardized Document used in the process of certifying a SCI Facility (SCIF). 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 (HVAC) connections, and security equipment layout. It shall also include any Waiver information.
For Official Use Only (FOUO)	A Dissemination Control Marking applied to Unclassified Information when Disclosure to the public of that particular Record, or portion thereof, would reasonably be expected to cause a foreseeable harm to an interest protected by one or more Exemptions of the Freedom of Information Act (FOIA).
Force Protection (FP)	Security programs designed to protect Service members, civilian Employees, family members, Facilities, information, and equipment in all locations and situations, accomplished through the planned and integrated application of Combating Terrorism, Physical Security, Operations Security, personal protective services, and supported by intelligence, counterintelligence, and Security programs.
Force Protection Condition (FPCON)	This term is no longer in use. ***Synonym(s)***: Terrorist Force Protection Condition
Foreign Contact	Contact with any person or entity that is not a U.S. Person.

Foreign Disclosure	The act of conveying information, in any form or manner, to an authorized representative of a foreign government or international organization without providing a copy for retention.
Foreign Disclosure Officer (FDO)	***Synonym(s)*:** Designated Disclosure Authority
Foreign Disclosure System (FDS)	An automated repository that provides DoD decision makers historical information to assist in making subsequent decisions regarding Foreign Disclosures of classified military information (CMI).
Foreign Entities	Foreign governments, international organizations, and coalition partners consisting of sovereign states, or others as determined by the DNI.
Foreign Government Information	(1) Information provided to the U.S. Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence. (2) Information produced by the U.S. Government 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. (3) Information received and treated as Foreign Government Information pursuant to Executive Order.
Foreign Government Official	As a nonimmigrant class of admission, an Alien coming temporarily to the U.S. who has been accredited by a foreign government to function as an ambassador, public minister, career diplomatic or consular officer, other accredited official, or an attendant, servant or personal employee of an accredited official, and all above Aliens' spouses and unmarried minor (or dependent) children.

Foreign Intelligence (FI)	Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence except for information on International Terrorism.
Foreign Interest	(1) Any foreign government, agency of a foreign government, or representative of a foreign government. (2) Any form of business enterprise or legal entity organized, chartered or incorporated under the laws of any country other than the United States or its territories. (3) A Foreign National.
Foreign Liaison Official	Foreign officials involved in liaison activities with U.S. Government officials.
Foreign National	Any person who is neither a United States Citizen nor a National of the United States. ***Synonym(s)***: Alien
Foreign Ownership, Control, or Influence (FOCI)	Factors considered in the aggregate as part of the CSA's determination of a contractor's eligibility for a facility security clearance based on their responses to questions on the Standard Form (SF) 328 (e.g., foreign ownership, foreign subsidiaries, foreign contracts, etc.) and the CSA's consideration of other factors stated in the National Industrial Security Program Operating Manual (NISPOM). See Under FOCI: A U.S. company for which a Foreign Interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable, through ownership of the U.S. company's securities, by contractual arrangements or other means, 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 affect adversely the performance of Classified Contracts.

Foreign Power	(1) A foreign government or any component thereof, whether or not recognized by the United States. (2) A faction of a foreign nation or nations, not substantially composed of United States Persons. (3) An entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments. (4) A group engaged in International Terrorism or activities in preparation therefor. (5) A foreign-based political organization, not substantially composed of United States Persons. (6) An entity that is directed and controlled by a foreign government or governments. (7) An entity not substantially composed of United States Persons that is engaged in the international proliferation of Weapons of Mass Destruction (WMD).
Foreign Release	The provision of Unclassified or Classified Information, whether in writing or any other medium, to authorized foreign recipients for retention.
Foreign Travel	Any travel outside the 50 United States and its territories.
Foreign Travel Briefing	A security briefing given to a person with Access to Classified Information who intends to travel outside the U.S. and its territories. ***Related Term(s)***: Defensive Security Briefing
Formerly Restricted Data (FRD)	Information removed from the Restricted Data (RD) category upon a joint determination by the DOE (or antecedent agencies) and the DoD that such information relates primarily to the military utilization of atomic weapons and that such information can be safeguarded adequately as classified defense information. For purposes of foreign dissemination, this information is treated in the same manner as Restricted Data (RD).
Full Scope Polygraph	This term in no longer in use. ***Synonym(s)***: Expanded-Scope Screening

General Security Agreement	An international agreement negotiated in diplomatic channels requiring each party to agree to afford Classified Information provided by the other party substantially the same degree of security protection afforded to the information by the providing party. Some of the agreements cover all Classified Information exchanged by the parties and are referred to generally as general security of information agreements, while others are limited to classified military information (CMI) and are referred to as general security of military information agreements.
Government-to-Government Principle	The principle that the Foreign Disclosure or export of classified military information (CMI) and Controlled Unclassified Information (CUI) is based on a decision that the information is authorized for Foreign Disclosure or export to the government or international organization of the intended recipient or end-user.
GSA Approved Field Safes	Portable Safes, approved by GSA in accordance with Federal specifications, that are uniquely made for military units for storage of classified material in the field.
Handling Instructions	Control Markings that restrict the Control Channels in which the information must be restricted, as in "Handle via <Compartment> Channels Only." This practice is being retired. ***Related Term(s)***: Control Marking
Hazard	Environmental, versus man-made, factors or events with the potential to cause damage to or loss of an Asset.
Head of Intelligence Community Element (HICE)	The head of an organization within the Intelligence Community (IC), or a designated representative. HICE replaces the term Senior Official of the Intelligence Community (SOIC), now obsolete. ***Synonym(s)***: Senior Official of the Intelligence Community

Historical Records Restricted Data Reviewers Certification (HRRDR)	Formal course, with a required examination, taught by the Department of Energy (DOE) providing instruction on proper identification of potential Restricted Data (RD) and Formerly Restricted Data (FRD) information. HRRDR certification is required by statute for all personnel conducting Automatic Declassification review. Half-day refresher training is required every five years.
Homeland Security (HS)	A concerted national effort to (1) prevent terrorist attacks within the U.S.; (2) reduce America's vulnerability to terrorism, major disasters, and other emergencies; and (3) minimize the damage and recover from attacks, major disasters, and other emergencies.
Identification and Markings	At the time of Original Classification, the following shall be indicated in a manner that is immediately apparent: one of the three Classification Levels (Confidential, Secret, or Top Secret); the identity, by name and position, or by personal identifier of the Original Classification Authority (OCA); the agency and office of origin; and Declassification instructions.
Identity	The set of attribute values (i.e., physical and behavioral characteristics) by which an individual is recognizable.

Identity Attributes	The authoritative reference of identity information for an individual (Biographical, contextual and biometric) that enables the verification of a claim of identity.
Identity information	Biographical, contextual, and biometric information that allows for the identification of an entity and determination of intent.
Identity Management (IdM)	The combination of technical systems, policies, and processes that creates, defines, governs, and synchronizes the ownership, verification, utilization, and safeguarding of Identity information.
Identify proofing	The process of reviewing sufficient information to authenticate an identity based on a review of authorized and acceptable documentation.
Immediate Family	The spouse, parents, siblings, children, and Cohabitant, including any step parents, half and step siblings, and step children of the Subject under investigation.
Immigrant Alien	***Synonym(s)*:** Lawful Permanent Resident
Impact	Within a Risk Management process, the amount of loss or damage to an Asset that can be expected in the event an Adversary compromises a known Vulnerability, and as may be influenced by time or other factors. ***Synonym(s)*:** Consequence
Indoctrination (Indoc)	Formal instruction to an individual approved for Access to SCI, a Controlled Access Program, or a SAP regarding program-unique information and program-specific security requirements and responsibilities. ***Synonym(s)*:** Read-On
Industrial Security	A multi-disciplinary security program concerned with the protection of Classified

	Information developed by or entrusted to U.S. industry.
Inestimable Damage	The capacity for harm too severe to be computed or measured.
Information Assurance (IA)	Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.
Information Security	The Security discipline concerned with implementation of a system of administrative policies and procedures for identifying, controlling, and protecting from Unauthorized Disclosure information that is authorized protection by Executive Order, statute, or regulation. Information Security includes protection of information that is Classified, Controlled Unclassified (CUI), and SCI.
Information Security Classification Appeals Panel (ISCAP)	The panel established to advise and assist the President in the discharge of his constitutional and discretionary authority to protect the National Security of the United States. ISCAP performs four critical functions: (1) deciding on appeals by any authorized person who has filed classification challenges permitted by Executive Order; (2) approving, denying, or amending agency Exemptions

	from Automatic Declassification; (3) deciding on Mandatory Declassification Review (MDR) appeals by parties whose requests have been denied at the agency level; and (4) deciding on agency requests to exempt a designated File Series from Automatic Declassification.
Infraction	A Security Incident involving failure to comply with established security requirements. Infractions cannot reasonably be expected to, and do not result in the loss or suspected or actual Compromise of Classified Information. Infractions may be unintentional or inadvertent. While they do not constitute Violations, if left uncorrected, they can lead to Violations or Compromises. ***Related Term(s):*** Security Incident
Ingress	Location in a perimeter, boundary, barrier, or designated Restricted Area that lends itself to an entry point from which Access to the Asset being protected can be gained.
Ingress Time	The sum of all time intervals required for an intruder to traverse from barrier to barrier within a site or Facility.
Inquiry	The fact-finding and analytic process conducted to determine whether a loss of Classified Information occurred, or whether unauthorized personnel had, or could have had, Access to the information.
Insider	Any Authorized Person with Access to any U.S. Government resource, to include personnel, Facilities, information, equipment, networks, or systems.
Insider Threat	The Threat that an Insider will use his/her authorized Access to do harm to the security of the U.S., including damage through espionage, terrorism, Unauthorized

	Disclosure of information, or through the loss or degradation of resources or capabilities
Inspectable Space	The three-dimensional space surrounding equipment that processes Classified Information within which TEMPEST exploitation is not considered practical, or where legal authority to identify and remove a potential TEMPEST exploitation exists when exercised. The Certified Tempest Technical Authority (CTTA) shall determine the inspectable space for a Facility.
Installation	A grouping of Facilities located in the same vicinity which support particular functions.
Intelligence Activities	All activities that Elements of the Intelligence Community (IC) are authorized to conduct pursuant to law or Executive Order.
Intelligence Disclosure Officer (IDO)	IC Element personnel to whom a Senior Foreign Disclosure Authority (SFDA) has delegated in writing the authority to approve or deny requests for authorization to Release or Disclose intelligence under that SFDA's jurisdiction or as authorized by Release related Control Markings. ***Related Term(s)***: Senior Foreign Disclosure Authority
Intelligence Special Access Program	A SAP established primarily to protect the planning and execution of especially sensitive intelligence or CI operations or collection activities. ***Related Term(s)***: Special Access Program
Intelligence Sources and Methods	Intelligence (1) Sources – Persons images, signals, Documents, databases, and communications media capable of providing intelligence through collection and analysis programs; e.g., Human Intelligence

	(HUMINT), Imagery Intelligence (IMINT), Signal Intelligence (SIGINT), Geospatial Intelligence (GEOINT), and Measurement and Signature Intelligence (MASINT); and (2) 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.
Interim Access	Access to National Security Information (NSI) based on the completion of minimum investigative requirements, which is granted on a temporary basis, pending the completion of the full investigative requirements.
Interim Access Authorization (IAA)	A determination to grant Access Authorization prior to the receipt and Adjudication of the individual's completed Personnel Security Investigation (PSI). ***Related Term(s)***: Temporary Access; Eligibility
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.
International Program	Any program, project, contract, operation, exercise, training, experiment, or other initiative that involves an IC Element, DoD Component, or a Contractor and a foreign government, international organization, or corporation that is located, or incorporated to do business, in a foreign country.
International Terrorism	Activities that (1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the U.S. or of any State, or that would be a criminal violation if committed within the jurisdiction of the U.S.

	or of any State; (2) appear to be intended to (a) intimidate or coerce a civilian population, (b) influence the policy of a government by intimidation or coercion, or (c) affect the conduct of a government by mass destruction, assassination, or kidnapping; and (3) occur primarily outside the territorial jurisdiction of the U.S., or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum.
Intrusion Detection System (IDS)	A Technical Security system designed to detect an attempted or actual unauthorized entry into a secure Facility or information system and to alert responders.
Investigation	***Synonym(s)***: Security Investigation
Investigative Record	The official Record of all data obtained on a Subject from a Trusted Information Providers, Suitability and or security applications and questionnaires, and any investigative activity conducted under these standards.
Investigative Service Provider (ISP)	An organization that conducts investigations.
Investigative Tier Standards	A range of standards for National Security and Suitability Investigations of all individuals seeking work or working for or on behalf of the Executive Branch of the Federal Government, and individuals with Access to federally controlled Facilities and information systems.
Issue Case	A case containing any Adverse Information, even if fully mitigated. ***Related Term(s)***: Adverse Information
Issue Information	***Synonym(s)***: Adverse Information

Joint Military Intelligence Program (JMIP)	This term is no longer in use. ***Synonym(s):*** Military Intelligence Program
Joint Personnel Adjudication System (JPAS)	The centralized DoD database of standardized Personnel Security processes. It virtually consolidates the DoD Central Adjudication Facilities by offering real time information concerning clearances, Access, and investigative statuses to authorized DoD security personnel and other interfacing organizations (e.g., Defense Security Service, Defense Manpower Data Center, Defense Civilian Personnel Management System, OPM, and the Air Force Personnel Center).
Jurisdiction	The limits within which authority can be exercised or asserted.
Key Card	A card used in conjunction with a Physical Access Control System (PACS) to limit Access to Controlled or Restricted Areas to authorized individuals. A Key Card does not necessarily identify the holder.
Key Resources	The publicly or privately controlled resources essential to the minimum operations of the economy and government. ***Related Term(s):*** Critical Infrastructure and Key Resources
Keying	The process of establishing a sequence of random binary digits used to initially to set up and periodically change permutations in cryptographic equipment for purpose of encrypting or decrypting electronic signals, for controlling transmission security processes, or for producing other keys.
Law Enforcement Sensitive (LES)	A Control Marking sometimes applied in addition to or in conjunction with the marking FOR OFFICIAL USE ONLY (FOUO), by the Department of Justice and other activities in the law enforcement community to denote that the information was compiled for law

	enforcement purposes and should be afforded appropriate security in order to protect certain legitimate government interests.
Lawful Permanent Resident (LPR)	A non-U.S. citizen who has been lawfully granted the privilege of residing and working permanently in the U.S. under the provisions of 8 USC § 1101. ***Synonym(s)***: Immigrant Alien; Permanent Resident Alien
Lead	A single investigative element of a case requiring action. Examples include reference interviews, record checks, Subject interviews, Local Agency Checks (LACs), state agency checks, consumer reporting agency checks, licensing checks, public records checks, and National Agency Checks (NACs).
Letter Of Compelling Need	A written statement by a program manager or designee declaring that the services of an individual with Eligibility issues (e.g., lacking U.S. citizenship or having Foreign National family members) are essential to mission accomplishment. ***Related Term(s)***: Compelling Need
Limited Access Area (LAA)	An area where entry is limited to personnel on an entry list. All other personnel entering must be on official business and be signed in and out on a Visitor's Register and escorted.
Limited Access Authorization (LAA)	Security Access authorization to Confidential or Secret information based on a favorable 10-year scope SSBI granted to non-U.S. citizens requiring such limited Access in the course of their regular duties.
Limited Background Investigation (LBI)	A moderate risk public trust Investigation that has five years of basic coverage to include three years of personal coverage. Leads of an LBI include a National Agency Check (NAC), credit check, education, employment,

	residence, law enforcement, court checks, and a personal interview. This practice is under review as part of the development of Investigative Tiered Standards, in which this practice would become a Tier 2 Investigation. ***Related Term(s)***: Investigative Tier Standards
Limited Distribution (LIMDIS)	A Control Marking used by National Geospatial-Intelligence Agency (NGA) to identify a select group of sensitive, Unclassified imagery or geospatial information and data created or distributed by NGA or information, data, and products derived from such information.
Limited Exception	See Exception (Physical Security).
Local Agency Check (LAC)	A review of the appropriate criminal history and court records in the jurisdictions over the areas where the Subject of Investigation has resided, attended school, or been employed during a specific period of time. ***Synonym(s)***: Local Law Enforcement Check
Local Law Enforcement Check	***Synonym(s)***: Local Agency Check
Lock	A device that meets GSA-approved standards and is used to delay unauthorized entry .
Locked Container	A container or room of substantial construction secured with a GSA-approved locking device. ***Related Term(s)***: Vault; Safe
Logical and Physical Access	Access other than occasional or intermittent to federally controlled Facilities or information systems.
Logical Access	Access to an organization information system by a user (or process acting on behalf of a user) communicating through a direct connection. Use of a credential to access information technology systems.

Loss of Jurisdiction	Loss of authority by an investigative or adjudicative agency to conduct Personnel Security Investigations (PSIs) or render Suitability or Eligibility determinations in cases where the association between an individual and the department or agency sponsoring the request has been terminated.
Mandatory Declassification Review (MDR)	A written request by any individual or organization for Declassification of information classified under Executive Order.
Marking	***Synonym(s)*: Overall Classification Marking** ***Related Term(s):*** Control Marking; Banner Marking
Material, Intentional False Statement	A statement capable of influencing, affecting, or having a natural tendency to affect an official decision, even if an agency does not rely on it. ***Related Term(s)*:** False Statement
Military Intelligence Program (MIP)	Programs, projects, or activities that support the Secretary of Defense's intelligence, counterintelligence, and related intelligence responsibilities. This includes those intelligence and counterintelligence programs, projects, or activities that provide capabilities to meet warfighters' operational and tactical requirements more effectively. The term excludes capabilities associated with a weapons system whose primary mission is not intelligence. ***Related Term(s)*:** National Intelligence Program ***Synonym(s)*:** Joint Military Intelligence Program (JMIP); Tactical Intelligence and Related Activities (TIARA)
Military Working Dog (MWD)	***Synonym(s)*:** Working Dog

Minimum Background Investigation (MBI)	A moderate risk public trust Investigation that covers the past five years of an individual's life. Leads include National Agency Check (NAC), credit check, education, employment, residence, law enforcement, court checks, and a Personal Security Interview. This practice is under review as part of the development of Investigative Tiered Standards, in which this practice would become a Tier 2 Investigation. ***Related Term(s)***: Investigative Tier Standards
Minor Adverse Information	See Adverse Information.
Mitigating Information	Personnel Security information that tends to explain or refute factors that could otherwise support Denial, Revocation, or the granting of Access only with an Exception.
Mosaic Effect	***Synonym(s)***: Compilation
Multiple Facility Organization (MFO)	A legal entity (sole proprietorship, partnership, association, trust, or corporation) composed of two or more Contractors.
National Agency Check (NAC)	An investigative process that queries, at a minimum, the OPM Security/Suitability Investigations Index (SII), FBI fingerprint records, and the DoD Clearance & Investigations Index (DCII). Depending upon the Subject's background, other U.S. Government, commercial or private organizations, and related databases may be queried.
National Agency Check with Inquiries (NACI)	A Personnel Security Investigation (PSI) combining a National Agency Check (NAC) and written inquiries to law enforcement agencies, former employers and supervisors, references, and schools.

National Agency Check With Local Agency Checks And Credit Check (NACLC)	A Personnel Security Investigation (PSI) covering the immediate preceding five to seven years and consisting of a National Agency Check (NAC), financial review, verification of date and place of birth, and Local Agency Checks (LAC).
National Crime Information Center (NCIC)	A computerized index of criminal justice information available to Federal, State, local law enforcement, and other criminal justice agencies that includes criminal record history information on fugitives, stolen properties, and missing persons.
National Declassification Center Reviewer Certification (NDC)	Formal modular course, with a required final examination and practicum, developed, maintained and taught by the NDC providing instruction on working with classified NARA Accessioned Records requiring Automatic Declassification Review.
National Disclosure Policy (NDP)	Promulgates national policy and procedures in the form of specific Disclosure criteria and limitations, definitions of terms, Release arrangements, and other guidance required by U.S. departments and agencies having occasion to Release Classified Information. In addition, it establishes and provides for the management of an interagency mechanism and procedures that are required for the effective implementation of the policy.
National Foreign Intelligence Board (NFIB)	An organization to oversee security and intelligence matters of the U.S., composed of representatives from IC Elements, chaired by the DNI, and established in accordance with the National Security Act of 1947, as amended.

National Industrial Security Program (NISP)	The program established by Executive Order to serve as the unified Industrial Security program throughout the Federal Government to protect classified information that may be, or has been, Released to current, prospective, or former Contractors, licensees, or grantees of the U.S. agencies, and to preserve U.S. economic and technological interests.
National Intelligence	All intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that pertains, as determined consistent with any guidance issued by the President, or that is determined for the purpose of Access to information by the DNI to pertain to more than one United States Government agency; and that involves threats to the United States, its people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on United States National or Homeland Security.
National Intelligence Program (NIP)	All programs, projects, and activities of the IC, as well as any other programs of the IC designated jointly by the DNI and the head of a U.S. department or agency, or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by U.S. Armed Forces. ***Related Term(s)***: Military Intelligence Program
National Interest Determination	Determination that Access to proscribed information is consistent with the National Security interests of the United States.
National of the United States	***Related Term(s)***: United States Citizen ***Synonym(s)***: United States National
National Security	The national defense or foreign relations of the United States.

National Security and Public Trust Position	A position that involves activities of the Government concerned with the protection of the nation from foreign aggression or espionage, including development of defense plans or policies, intelligence or counterintelligence activities, and related activities concerned with the preservation of the military strength of the U.S.; including, but not limited to, positions that require regular use of, or Access to, Classified Information. Such positions are designated as Non-Sensitive, Non-Critical Sensitive, Critical-Sensitive, or Special-Sensitive. ***Synonym(s)***: Sensitive Position ***Related Term(s)***: Public Trust Position
National Security Information (NSI)	Information that has been determined pursuant to Executive Order to require protection against Unauthorized Disclosure and that is so designated. ***Related Term(s)***: Classified Information
National Security Special Event (NSSE)	A designated event that, by virtue of its political, economic, social, or religious significance, may be the target of terrorism or other criminal activity.
National Security Strategy (NSS)	A Document approved by the President of the United States for developing, applying, and coordinating the instruments of national power to achieve objectives that contribute to National Security.
NATO Information	Information generated by or for NATO, or member nation national information that has been released into the NATO security system.
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 within the Executive Branch in accordance with directives issued pursuant to Executive Order that a prospective recipient requires Access to specific Information in order to perform or assist in a lawful and authorized governmental function.
Newly Discovered Records	Records that were inadvertently not reviewed prior to the effective date of Automatic Declassification because the appropriate agency personnel were unaware of their existence.
Nickname	A combination of two separate Unclassified words that is assigned an Unclassified meaning and is employed only for Unclassified administrative, morale, or public information purposes.
No Deception Indicated (Polygraph) (NDI)	A favorable opinion regarding the outcome of an issue-based Polygraph Examination based upon test data analysis for all the relevant questions in a completed test series. ***Synonym(s)*:** No Significant Physiological Responses (Polygraph)
No Opinion (Polygraph) (NO)	An opinion regarding the outcome of a polygraph or PCASS test series, or overall examination result, when there is insufficient physiological data for conclusive test data analysis. For statistical purposes, a case may be considered as a NO when an examinee withdraws consent to undergo testing before physiological data can be obtained.
No Significant Physiological Responses (Polygraph) (NSP)	***Synonym(s)*:** No Deception Indicated (Polygraph)
No Specific Response (Polygraph) (NSR)	A favorable opinion regarding the outcome of a security Screening Polygraph or PCASS examination based upon test data analysis for all the relevant questions in a completed test series.

Non-Accountable SCI	SCI that does not require a Document Accountability Number (DAN) for traceability, retrieval, and audit of material.
Noncritical-Sensitive Positions	Positions with the potential to cause damage to the National Security up to and including damage at the significant or serious level. Such positions include: (1) Access to Secret, "L," or Confidential Classified Information; (2) Any other positions with the potential to cause harm to National Security to a moderate degree that do not rise to the level of the Critical-Sensitive or Special-Sensitive Positions. ***Related Term(s)***: Sensitive Position
Nondisclosure Agreement (NdA)	A contractual agreement between the U.S. Government and a cleared Employee, in which the Employee agrees never to disclose Classified Information to an unauthorized person. Its primary purpose is to inform a cleared employee of (1) the trust that is placed in them by providing them Access to Classified Information; (2) their responsibilities to protect that information from Unauthorized Disclosure; and (3) the consequences that may result from their failure to meet those responsibilities.
Non-Discussion Area	A defined area within a SCI Facility (SCIF) where classified discussions are not authorized.
Non-Sensitive Position (NS)	A position with the potential for impact on the integrity or efficiency of the service, but very little impact on the National Security. ***Related Term(s)***: Sensitive Position
NSA/CSS Secure Telephone System (NSTS)	A dedicated, automatic, self-authenticating secure voice network established and maintained to facilitate the cryptologic mission of the National Security Agency /Central Security Service (NSA/CSS).
Open Post	Access to the installation or activity is not controlled during or after normal duty hours.

Open Source	Unclassified verbal, documentary, pictorial, or physical material Accessible to the public.
Open Storage	The storage of information or information systems that are Classified, or Controlled Unclassified (CUI) in an approved secure space whereby the space is the secure container and may be unoccupied by authorized personnel when the material is not in use.
Open Storage Area	A space constructed in accordance with established standards and authorized by the agency head or designee as meeting the requirements for Open Storage of information or information systems that may be Classified, or Controlled Unclassified (CUI).
Operations & Maintenance (O&M)	An appropriation budget category composed of many appropriation titles that traditionally finance those things whose benefits are derived for a limited period of time; i.e., expenses, rather than investments.
Operations and Support Special Access Program	**A SAP established primarily to protect the planning for, execution of, and support to especially sensitive military operations. An operations and support SAP may protect organizations, property, operational concepts, plans, and activities.** ***Related Term(s)*:** Special Access Program
Operations Security (OPSEC)	A process of identifying critical information and analyzing friendly actions attendant to military operations and other activities to: identify those actions that can be observed by adversary intelligence systems; determine indicators and vulnerabilities that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and determine which of these represent an unacceptable risk; then select and execute countermeasures that eliminate the risk to friendly actions and operations or

	reduce it to an acceptable level.
OPSEC assessment	An evaluation process of an organization, operation, activity, exercise, or support function to determine if sufficient countermeasures are in place to protect critical information.
OPSEC indicator	Friendly detectable actions and open source information that adversaries can interpret and piece together to derive critical or classified information concerning friendly intentions, capabilities, or activities.
OPSEC survey	An application of the OPSEC process by a team of subject matter experts to conduct a detailed analysis of activities associated with a specific organization, operation, activity, exercise, or support function by employing the known collection capabilities of potential adversaries.
Original Classification	An initial determination that information requires, in the interest of the National Security, protection against Unauthorized Disclosure.
Original Classification Authority (OCA)	An individual authorized in writing, either by the President, the Vice President, agency heads or other officials designated by the President, to classify information in the first instance.
Originating Agency	***Synonym(s)*:** Originator
Originating Agency's Determination Required (OADR)	An obsolete Control Marking signifying that the Originator must approve any Declassification action.
Originator	The agency that possesses and exercises Classification Authority (Original or Derivative) over the information. ***Synonym(s)*:** Originating Agency
Outgoing Visit Request (OVR)	***Synonym(s)*:** Visit Authorization Request
Overall Classification Marking	The practice of noting the Classification Level of the Document as a whole at the top

	and bottom of each page (the header and footer) with the highest Classification Level of information found in any portion of the Document.
Overseas Security Policy Board (OSPB)	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 U.S. Government agencies under the authority of a Chief of Mission.
Page Marking	The marking at the top (header) and bottom (footer) of each page of a classified Document that specifies both the highest Level of Classification of information contained on that page and the most restrictive Control Marking(s) applicable. ***Related Term(s):*** Banner Line
Parent Corporation	A corporation that owns at least a majority of another corporation's voting securities.
Particularly Sensitive Classified Information	Information about (1) the identity of covert agents, intelligence collection, and processing systems; (2) certain cryptographic systems and equipment; (3) particularly sensitive SAPs; and (4) especially sensitive nuclear weapons design information. ***Related Term(s):*** Financial Disclosure Program
Perimeter Control	Objects and measures deployed to establish physical boundaries such as barriers, fences, and natural barriers.
Period of Investigation	The time covered during the Investigation, calculated by using the investigative Scope required by the type of Investigation, plus other pertinent factors such as the age of the applicant or the date of the last Investigation.
Periodic Reinvestigation (PR)	The administrative reinvestigation at set intervals of individuals with Access to classified information, performed to ensure

	the person continues to be eligible to remain in their position or have Access to Classified Information.
Permanent Certification (Perm-Cert)	A certification of a person's Access(es) to another organization or Facility for a specific period, not to exceed three years.
Permanent Exception	See Exception (Physical Security).
Permanent Record	***Synonym(s)***: Record with Permanent Historical Value
Permanent Resident Alien (PRA)	***Synonym(s)***: Lawful Permanent Resident
Permanently Valuable Information	***Synonym(s)***: Record with Permanent Historical Value
Personal Coverage	(1) An investigative coverage method wherein face-to-face interviewing takes place.
Personal Electronic Devices	Personally-owned electronic devices having the capability to store, record, or transmit text, images, video, or audio data. ***Related Term(s)***: Portable Electronic Devices
Personal Financial Statement (PFS)	The form used as part of a Personnel Security Investigation (PSI) to provide a summary of a person's total monthly income, debt payments, expenses, and net remainder of income.
Personal Identity Verification Card (PIV Card)	A physical artifact conforming to Federal standards issued by the Federal, state or local government to an individual that contains a photograph, cryptographic keys, and a digitized fingerprint representation so that another person or an automated process can verify the claimed identity of the cardholder. ***Related Term(s)***: CAC Card
Personally Identifiable Information (PII)	Information that can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place

	of birth, mother's maiden name, and biometric records containing personal information which is linked or linkable to a specific individual.
Personnel Reliability Program (PRP)	A program designed to ensure the highest possible standards of individual reliability in personnel performing duties associated with nuclear weapons systems and critical components.
Personnel Security	The security discipline that assesses the loyalty, reliability, and trustworthiness of individuals for initial and continued Eligibility for Access to Classified Information or assignment in Sensitive Positions.
Personnel Security Appeals Board (PSAB)	The review board that decides appeals of Unfavorable Personnel Security Determinations made by an Authorized Adjudicative Agency (AAA).
Personnel Security Clearance (PCL)	A privilege granted to an individual to gain Access up to a specified level of classified information who: (1) is deemed by an Authorized Adjudicative Authority to be eligible for Access to Classified Information; (2) is required by assigned duties to such Access; and (3) has signed an Nondisclosure Agreement (NdA). ***Related Term(s)***: Security Clearance ***Synonym(s)***: Clearance
Personnel Security Interview	An interview conducted with an applicant for a Security Clearance or a person with current eligibility to discuss areas of security relevance. ***Synonym(s)***: Subject Interview
Personnel Security Investigation (PSI)	National Security and Suitability Investigations of all individuals seeking work or working for or on behalf of the Executive Branch of the Federal Government, and individuals with Access to federally controlled Facilities and information systems.

	Related Term(s): Security Investigation ***Synonym(s)***: Background Investigation; Special Background Investigation
Personnel Security Questionnaire (PSQ)	Security forms, whether paper or electronic, completed as part of a Personnel Security Investigation (PSI) for National Security Positions
Phased Periodic Reinvestigation (PPR)	A Periodic Reinvestigation (PR) that may exclude references and neighborhood check requirements when no information of security concern is developed through the other reinvestigation requirements. ***Related Term(s)***: Periodic Reinvestigation
Physical Access	Vehicle and pedestrian access to DoD or Federally controlled installations, facilities, and other locations. Access may be escorted or unescorted.
Physical Access Control	***Synonym(s)***: Access Control
Physical Access Control System (PACS)	***Synonym(s)***: Access Control System
Physical Security	Security concerned with physical measures designed to safeguard personnel, prevent unauthorized access to equipment, installations, material, and documents, and defend them against espionage, sabotage, damage, and theft.
Physical Security Equipment	A generic term encompassing any item, device, or system that is used primarily for the protection of Government property, including nuclear, chemical, and other munitions; for the protection of personnel, and Installations, and safeguarding classified information and material, including the destruction of such information and material both by routine means and by emergency destruct methods.
Physical Security Inspection	A formal, recorded process by which the economy, efficiency, effectiveness, and accountability in the management of Physical

	Security Measures is assessed.
Physical Security Measures	The physical and electronic hardware, software, equipment, accessories, and human measures designed to (1) protect personnel; (2) prevent unauthorized Access to Facilities, equipment, material, and Documents; and (3) defend against espionage, terrorism, sabotage, damage, or theft.
Physical Security Plan	A comprehensive written plan detailing the personnel, procedures, and equipment in use at a Facility or site to prevent or minimize loss or damage of property, Assets, and information from theft, misuse, espionage, sabotage, and other criminal or disruptive activities.
Polygraph Examination	(1) The use of the Polygraph Instrument with respect to an examinee. (2) Any questioning or other processing involving the examinee before or after the use of the polygraph. ***Related Term(s)*:** Preliminary Credibility Assessment Screening System / Instrument
Polygraph Instrument	A diagnostic instrument to measure and record respiration, electrodermal, blood volume, and heart rate responses to verbal or visual stimuli.
Portable Electronic Devices (PEDs)	U.S. Government-issued wireless electronic devices having the capability to store, record, or transmit text, images, video, or audio data. ***Related Term(s)*:** Personal Electronic Devices
Portion Marking	The practice of noting the Classification Level and Control Markings of each information element (e.g., paragraph, subject, title) in a Document.

Position Designation	The assessment of the potential for adverse Impact on the integrity and efficiency of the service, or the assessment of the degree to which, by the nature of the position, the occupant could bring about a material adverse effect on the National Security.
Position Risk Evaluation	The assessment of the potential Risk to the integrity or efficiency of the service of higher Public Trust Positions as part of the Suitability evaluation process.
Practice Dangerous to Security (PDS)	A failure to comply with the provisions of security regulations which has the potential to cause a Compromise of Classified Information.
Preliminary Credibility Assessment Screening System / Instrument (PCASS)	A diagnostic instrument used during an interview capable of monitoring, recording, and/or measuring electrodermal and vasomotor activity. ***Related Term(s)*:** Polygraph Instrument; Polygraph Examination
Presidential Records	The papers or records of the former Presidents under the legal control of NARA pursuant to the Presidential Records Act. ***Related Term(s)*:** Record; Federal Records
Primary Activity	The activity, such as employment, education, or unemployment, in which the Subject of an Investigation is primarily engaged.
Prime Contract	A contract let by a Government Contract Authority (GCA) to a Contractor for a legitimate government purpose.
Prime Contractor	The Contractor who receives a Prime Contract from a Government Contract Authority (GCA).
Principal Disclosure Authority (PDA)	A senior military or civilian government official appointed in writing by the head of an OSD organizational element or a DoD Component as the Senior Foreign Disclosure Authority (SFDA), responsible for the

	establishment of a Foreign Disclosure program consistent with DoD standards.
Privileged User	An individual who has Access to system control, monitoring, or administration functions (e.g., system administrator, system information system security officer, maintainers, or system programmers).
Program Disestablishment	The action taken when active enhanced protective measures are no longer required for the information contained within the program. ***Related Term(s)***: Special Access Program
Program Identifier (PID)	An unclassified three-letter acronym or abbreviated identifier for an assigned SAP nickname or code word. ***Related Term(s)***: Special Access Program
Program Termination	A SAP, compartment, or project whose activities have ceased and will not be restarted. SAP security measures are still required. ***Related Term(s)***: Special Access Program
Program Transition	An action that results in a change in protection level for the SAP material such as SAP to non-SAP, classified to unclassified, or the transfer of information to another SAP or compartment. ***Related Term(s)***: Special Access Program
Proscribed Information	Information that is: Top Secret; Communications Security (COMSEC) material, excluding Controlled Cryptographic Items (CCI) when unkeyed or utilized with Unclassified keys; Restricted Data (RD); SAP; or SCI.
Prospective Special Access Program (PPSAP)	A program or activity for which enhanced security measures have been proposed and approved to facilitate security protections prior to establishing the effort as a SAP.

Protected Distribution System (PDS)	A wire line or fiber optics telecommunications system with adequate electrical, electromagnetic, and physical Safeguards to permit its use for the transmission of unencrypted information through lesser-classified or uncontrolled areas.
Protection in Depth	A system providing several supplementary security barriers. For example, a perimeter fence, a secure building, a Vault, and a Locked Container provide four layers of Protection in Depth. ***Related Term(s)***: Security-in-Depth
Protective Detail	Armed personnel protection and security support provided to certain identified Government Employees and foreign dignitaries.
Protective Layer	Any envelope of building components which surrounds an Asset and delays or prevents aggressor movement toward the Asset or which shields the Asset from weapons and explosives effects.
Public Key Infrastructure (PKI)	The framework and services that provide for the generation, production, distribution, control, accounting and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates.
Public Trust Position	Positions at the high or moderate Risk levels that involve policy making, major program responsibility, public safety and health, law enforcement duties, fiduciary responsibilities or other duties demanding a significant degree of public trust, and positions involving Access to or operation or control of financial records,

	with a significant risk for causing damage or realizing personal gain. ***Related Term(s)***: National Security and Public Trust Positions
Publicly Available Information	Information that has been published or broadcast for public consumption, is Accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public. ***Related Term(s)***: Open Source
Random Antiterrorism Measures (RAM)	A systematic approach to developing random, multiple security measures that consistently change the look of an Installation's security posture designed to introduce uncertainty to defeat surveillance attempts and make it difficult for a terrorist to accurately predict actions.
Random Procurement	The acquisition by Top Secret cleared U.S. Citizens of existing local off-the-shelf stock without pre-announcement or referral that is immediately transported for use in the new construction, modification, or provisioning of an existing SCIF Facility (SCIF) or Secure Work Area (SWA).
Random Selection	The process of selecting a portion of building materials from bulk shipment procured for non-specific general construction use and not authorized for a SCI Facility (SCIF) or a Secure Work Area (SWA).
Re-accreditation	The formal Certification by a Cognizant Security Authority (CSA) that a Facility, designated area, or information system has been re-evaluated based upon the most current DNI security standards and has been

	approved to continue handling, processing, discussing, disseminating or storing SCI.
Read-Off	***Synonym(s)***: Termination Security Briefing
Read-On	***Synonym(s)***: Indoctrination
Reciprocity	Interagency recognition and acceptance of: a) background investigations and clearance eligibility determinations; b) accreditations of information systems; and c) facility accreditations.
Reclassification	The act of classifying information that was previously declassified under proper authority.
Record	A Document created or received and maintained by an agency, organization, or individual in pursuance of legal obligations or in the transaction of business. ***Related Term(s)***: Federal Records; Presidential Records ***Synonym(s)***: Document
Record with Permanent Historical Value	Information contained in: (1) Records that have been Accessioned by the National Archives; (2) Records that have been scheduled as permanent under a Records disposition schedule approved by NARA; and (3) Presidential historical materials, Presidential Records or donated historical materials located in the National Archives, a presidential library, or any other approved repository. ***Synonym(s)***: Permanently Valuable Information; Permanent Record ***Related Term(s):*** Presidential Records
Records Management	The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to Records creation, maintenance, use, and 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.

Reference

A person identified as having knowledge of the Subject of a Personnel Security Investigation (PSI). References are characterized by source and by type. There are two sources, those listed by the Subject on the Personnel Security Questionnaire (PSQ), and those developed by the investigator in the course of pursuing leads. There are six types pertaining to education, employment, co-workers, neighbors, friends or associates, and other persons who know the subject in some other context.
Related Term(s): Personnel Security Investigation

Referral

In Classification Management, information, in the possession of an organization that did not originate it, that requires review by the owner or subsequent authority to determine whether it can be Declassified or Released to the public. For Automatic Declassification, a Referral is Classified Information that was originated by or would affect the interest of another agency and could reasonably be expected to fall under one or more of the Automatic Declassification Exemptions.

Refresher Briefing

The Periodic Re-indoctrination on the National Security Information (NSI) program provided to personnel with continuing authorized Access to Classified Information.

Reinstatement

A process whereby an individual whose Access Authorization has been Terminated, Suspended, or Revoked is permitted to regain Access to Classified Information.

Reinvestigation

An Investigation conducted to update a previously completed Personnel Security Investigation (PSI).

Release

The provision of classified information, whether in writing or any other medium, to

	authorized recipients for retention.
Reliable Human Review	The process whereby an individual who is authorized to conduct a manual review of information, and possesses adequate knowledge and understanding of the information, makes an informed decision on the appropriate Classification Level.
Research, Development, and Acquisition Protection	The safeguarding of selected research, technology, information, and associated support systems, during the research, development, test, and evaluation and acquisition processes.
Response	The physiological change to the applied stimulus. Recommend qualifying this somehow. Responses are discussed in background investigations, forms, and all other kinds of contexts beyond stimulus-response contexts.
Resources	Personnel and/or materiel provided as a means of support (excludes funds/monies in this context)
Responsible Agency	The agency possessing Classification, Declassification, Release authority (whether domestic or foreign), or Records Management duties for information under its Control, or in which it has Equity. A Responsible Agency may or may not be the Originating Agency, and may be a successor organization gaining Control or Equity as a result of a transfer of function from, or wholesale dissolution of, the Originating Agency. ***Related Term(s):*** Equity; Control ***Synonym(s):*** Data Owner; Equity Holder
Restricted Area	An area (land, sea or air) in which there are special restrictive measures employed to prevent or minimize incursions or interference, where special security measures are employed to prevent unauthorized entry.
Restricted Data (RD)	All data concerning design, manufacture, or utilization of atomic weapons; the production

	of special nuclear material; or the use of special nuclear material in the production of energy, but not data declassified or removed from the RD category pursuant to the Atomic Energy Act of 1954, as amended.
Revocation	(1) An adjudicative decision to remove an individual's Access to classified information, material, Facilities, or Suitability for employment in a Sensitive Position, for cause. (2) An administrative decision to remove a Facility Accreditation or Clearance (FCL) for cause, thus terminating the capability to discuss, process, or store classified information,. ***Related Term(s):*** Security Clearance; Facility Clearance
Risk	A measure of consequence of peril, hazard or loss, which is incurred from a capable aggressor or the environment (the presence of a threat and unmitigated vulnerability).
Risk Analysis	The analytic method used to conduct a Risk Assessment.
Risk Assessment	A process which evaluates Threat(s) to, and Vulnerabilities of, an Asset to determine the probability of loss or damage, and its Impact.
Risk Management	The process that includes a critical evaluation of Threats, Vulnerabilities, and Assets to determine the need and value of Countermeasures.
Risk Management Principles	The principles applied for assessing Threats and Vulnerabilities and implementing security Countermeasures while maximizing the sharing of information to achieve an Acceptable Level of Risk at an acceptable cost.
Risk of Capture Briefings	Advisories that alert personnel as to what may be expected in the way of attempts to force or trick them to divulge Classified Information if captured or detained and that offer suggested

	courses of action they should follow to avoid or limit such divulgence. These advisories include instructions and advice for advance preparation of innocuous, alternate explanations of duties and background.
Routine Use	With respect to the Disclosure of a Record, the use of such Record for a purpose which is compatible with the purpose for which it was collected.
Sabotage	Sabotage means the willful destruction of government property with the intent to cause injury, destruction, or defective production of national defense or war materials by either an act of commission or omission.
Safe	A substantial, secure container with varying degrees of security or fire resistance, used to store valuables or classified information against fire, unauthorized Access, or theft. ***Related Term(s)***: Locked Container
Safeguard	The use of measures and controls to protect Classified or Controlled Unclassified Information (CUI).
Sanitization	(1)The altering, or removal, of Classified Information, property, or areas to permit wider dissemination or physical Access. (2) Removal of all classified information from electronic media.
Scattered Castles (SC)	The IC Security Clearance repository and authoritative source for Clearance and Access information for all IC, military services, DoD civilians, and Contractor personnel. ***Related Term(s)***: JPAS
SCI Access Determination Authority	***Synonym(s)***: Determination Authority
SCIF Co-Utilization	The mutual agreement among two or more Government organizations to share the same SCI Facility (SCIF).

Scope	The time period to be covered and the sources of information to be contacted during the prescribed course of a background investigation.
Screening	Reviewing a person's presented biographic and biometric information, as appropriate, to determine their authenticity, authorization, and Credential verification against an approved data source through authorized and secure channels anytime during the person's period of approved physical and/or logical Access. This assessment identifies Derogatory Information that can be determined as disqualifying issues for current or continuing Access to a resource, Asset, or Installation. ***Synonym(s)***: Vetting
Seal	A device or material that indicates tampering or entry. Seals are used to secure conveyance doors, intermodal container doors, and item shipping and storage container covers and lids.
Sealed Containers	Wooden boxes, crates, metal containers, and fiber containers sealed in a way to show when the containers are tampered with after sealing.
Secret (S)	See Classification Level.
Secure Facility	***Synonym(s)***: Secure Room
Secure Room	An area where Collateral Classified or Controlled Unclassified (CUI) discussions may be held or materials stored because appropriate Physical Security Measures are in place to guard against unauthorized disclosure. ***Synonym(s)***: Secure Facility
Secure Telephone Equipment (STE)	The next generation of secure voice and data equipment for advanced digital communication networks. The STE consists of a host terminal and a removable security core. The host terminal provides the application hardware and software. The

	security core provides all the Encryption and other security services.
Secure Telephone Unit (STU)	Dual-purpose telephone capable of transmitting and receiving voice and data. It may be used as an ordinary non-secure telephone with interoperability into the public telephone network or as a secure telephone, connectable through the public telephone network to other STU-III Type 1 (classified/sensitive use) or Type 2 (sensitive/Unclassified use only) telephones; or to a NSA/CSS Secure Telephone System (NSTS) telephone through the NSTS enclave.
Secure Working Area (SWA)	An Accredited Facility used for the discussion, handling, or processing SCI, but specifically not for the storage of SCI.
Security	Proactive measures employed to Safeguard personnel, information, operations, resources, technologies, Facilities, and other items deemed vital against harm, loss, or hostile acts and influences.
Security Assistance	A written confirmation, requested by and exchanged between governments representatives, that contains the following: (1) verification of the personnel Security Clearance level of the providing government's citizens or nationals; (2) a statement by a responsible official of the providing government that the recipient of the information is approved by the government for Access to information of the security classification involved on behalf of the government; (3) an obligation that the recipient government will ensure compliance with any security agreement or other security requirements specified by the U.S. Government.
Security Badge	***Synonym(s)***: Badge
Security Banner	A warning notice that the resource being Accessed contains classified material and

	must be protected as such.
Security Classification Guide	***Synonym(s)*:** Classification Guide
Security Clearance	A privilege granted to an individual to gain access up to a specified level of national security information who: a) is deemed by an authorized adjudicative authority to be eligible for access to national security information; b) has been deemed by an authorized individual to have a need for access; and c) has signed a Non-Disclosure Agreement.
Security Debriefing	***Synonym(s)*:** Termination Security Briefing
Security Debriefing Acknowledgement (CSA)	A statement signed by the individual reaffirming his or her continued responsibility to Safeguard Classified Information and the consequences of failing to do so, upon loss of Access either for the lack of Need For Access, or a change in the person's Eligibility qualifications as determined by the Cognizant Security Authority (CSA).
Security Engineering	The application of engineering principles to the protection of Assets from various Threats.
Security Environment Threat List (SETL)	A list of countries with U.S. Diplomatic Missions compiled by the Department of State and rated according to the following factors: (1) transnational terrorism; (2) indigenous terrorism; (3) political violence; (4) human intelligence; (5) technical threats; and (6) criminal threats. Each country is ranked at one of four levels: (1) Critical – definite Threats based on Adversary capability, intent to attack, and the targeting conducted on a recurring basis; (2) High – credible Threats based on knowledge of an Adversary's capability, intent to attack, and related incidents at similar facilities; (3) Medium – potential Threats based on 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; and (4) Low – little or no Threat as a result of the absence of credible evidence of capability, intent, or history of actual or planned attack against U.S. Assets.
Security Force	Personnel at an Installation or Facility tasked to provide Physical Security, Force Protection, or law enforcement.
Security Incident	An act or circumstance that constitutes a Threat to a security program or is a Deviation from existing governing security regulations. Security Incidents may be categorized as Infractions or Violations.
Security Investigation	(1) An in-depth, comprehensive examination to determine the facts and circumstances of a Violation and the presence, nature, and severity of any associated Compromise. (2) A Personnel Security Investigation (PSI) or Periodic Reinvestigation (PR) of a Subject for a Security Clearance, Suitability determination, or Access Credential. ***Synonym(s):*** Investigation
Security Manager	***Related Term(s):*** Security Professional
Security Office Identifier (SOI)	A four-character identifier assigned to an office designated to receive case results, data, or other information from Personnel Security or Suitability Investigations conducted by OPM.
Security Officer (SO)	***Related Terms(s):*** Security Professional
Security Procedural Measures	Physical Security measures to counter Risk factors that will periodically change over a period of time such as criminal, terrorist, and hostile Threats.

Security Professional	A functional career occupation in which the incumbent executes or manages Federal Government agency or Industrial Security programs and related security activities, ensuring compliance with government security policies, directives, and procedures. Examples of responsibilities and position titles include: Activity Security Manager, Chief Security Officer, Field Security Officer, Area Security Officer, Special Security Representative, Program Security Officer), and Security Guard. ***Related Term(s):*** Security Officer; Security Manager
Security Professional Education Development Program (SPeD)	A DoD initiative to professionalize the security workforce by ensuring there is a common set of competencies among security practitioners that promotes interoperability, facilitates professional development and training, and develops a workforce of certified Security Professionals.
Security/Suitability Investigations Index (SII)	An index established and maintained by OPM covering all persons for whom Personnel Security Investigations (PSIs), including those for Suitability, have been conducted by any department or agency of the Government. The index contains the name of each person investigated, adequate identifying information concerning each such person, and a reference to each department and agency which has conducted an Investigation concerning the person involved or has suspended or terminated the employment of such person.
Security-In-Depth	A combination of layered and complementary security controls sufficient to deter, detect, delay, and document unauthorized entry and movement within the Installation or Facility .
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 by Executive Order.
Senior Agency Official	The official designated by an agency head to

	direct and administer that agency's program under which information is Classified, Safeguarded, and Declassified.
Senior Foreign Disclosure Authority (SFDA)	The designated senior civilian or flag-rank official(s) within an IC Element responsible for that Element's Foreign Disclosure and Release program. ***Related Term(s)***: Intelligence Disclosure Officer ***Synonym(s)***: Designated Intelligence Disclosure Officer
Senior Official of the Intelligence Community (SOIC)	This term is no longer in use. ***Synonym(s)***: Head of Intelligence Community Element (HICE)
Sensitive but Unclassified Information (SBU)	Department of State information deemed to warrant protection and administrative control that meets the criteria for exemption from Freedom of Information Act (FOIA) Release.
Sensitive Compartmented Information (SCI)	See Controlled Access Program.
Sensitive Compartmented Information Facility (SCIF)	A formally accredited area, room, group of rooms, or Installation where SCI is stored, used, discussed, or electronically processed. SCIFs may be permanent or temporary, mobile or fixed, operating at U.S. Government-controlled Facilities, Contractor plants, or other civilian Installations.
Sensitive Compartmented Information Facility Database	The IC database that provides an integrated list of worldwide SCI Facilities (SCIFs) used to promote continuity of operations and relocation of affected resources in the event of a national emergency. ***Related Term(s)***: SCIF

	level of Investigation required for entry into the Federal service is the National Agency Check and Inquiries (NACI) Investigation. Persons appointed to Covered Positions must undergo an Investigation by OPM or by an agency conducting Investigations under delegated authority from OPM.
Supplemental Controls	Prescribed procedures or systems that provide security control measures designed to augment the physical protection of Classified Information. Examples of supplemental controls include Intrusion Detection Systems (IDS), and periodic inspections of security containers or areas.
Suspension of Access	The temporary withdrawal of a person's Access to classified information when information becomes known that casts doubt on whether continued Access is consistent with National Security interests. ***Synonym(s)***: Access Suspension
Systematic Declassification Review	The review for Declassification of Classified Information contained in Records that have been determined by NARA to have Permanent Historical Value in accordance with statute.
Tactical Approval To Operate (TAOP)	Cognizant Security Authority (CSA) delegated authority to an operational element to allow a Tactical SCI Facility (T-SCIF) to be functional before formal Accreditation is received.
Tactical Intelligence and Related Activities (TIARA)	This term is no longer in use. ***Synonym(s)***: Military Intelligence Program
Tactical SCIF (T-SCIF)	An area, room, group of rooms, building, or Installation accredited for SCI-level processing, storage, and discussion used for actual or simulated operational exigencies for a specified period of time not exceeding one year. ***Related Term(s)***: SCIF

Tearline	Portions of an intelligence report or product that provide the substance of a more highly classified or controlled report without identifying sensitive Intelligence Sources and Methods, or other operational information. Tearlines enable release of Classified Information with less restrictive Dissemination Controls, and when possible, at a lower Classification Level.
Tearline Reporting	An automated or manual technique for separating an intelligence report into multiple portions by machine- or human-readable markings, delimiting a sanitized version of more highly Classified or controlled information without identifying sensitive Intelligence Sources and Methods for the express purpose of permitting wider dissemination of the intelligence to authorized customers.
Technical Data	Technical information whose export to non-U.S. entities or countries is regulated by Federal export control because it is either inherently military in character or has both military and civilian uses.
Technical Deviation	A physical security condition that technically varies from policy standards, yet, affords the same level of protection. ***Synonym(s)***: Variance
Technical Security	A sub-discipline of Security dedicated to detecting, neutralizing, or exploiting a wide variety of hostile and foreign penetration technologies and requiring training in various Countermeasure techniques. ***Related Term(s)***: Technical Surveillance Countermeasures
Technical Security Assessment (TSA)	***Synonym(s)***: Technical Security Evaluation

Technical Security Evaluation (TSE)	An evaluation of all factors related to potential Vulnerabilities of technical penetration of a Facility, system, product or equipment. Typical considerations include security against acoustical, optical, audio frequency, and other methods of penetration as well as adequacy of electronic protection. A Technical Security Evaluation includes Technical Surveillance Countermeasures (TSCM) and TEMPEST considerations. ***Synonym(s)***: Technical Security Assessment
Technical Surveillance Counter-Measures (TSCM)	Physical, electronic, and visual techniques used to detect and counter technical surveillance devices, Technical Security Threats, and related Physical Security deficiencies.
Technical Surveillance Counter-Measures 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 Threats.
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.
TEMPEST (TEMPEST)	An Unclassified term that refers to the Investigation and study of Compromising Emanations.
TEMPEST Accreditation	Approval granted by the cognizant Certified TEMPEST Technical Authority (CTTA) to process Classified Information electronically based upon favorable evaluation or TEMPEST test results indicating compliance with the National Policy and Control of Compromising Emanations.

TEMPEST Addendum	An addendum to the Fixed Facility Checklist (FFC) that provides information to the Certified TEMPEST Technical Authority (CTTA) to aid in the determination of what TEMPEST Countermeasures, if any, need to be applied to a SCI Facility (SCIF).
Temporary Access	Eligibility for Access to Classified Information may be granted where there is a temporary need for Access provided the investigative standards required by Executive Order have been satisfied. A fixed date or event for expiration shall be identified and Access to Classified Information shall be limited to information related to the particular project or assignment. ***Synonym(s)***: Special Purpose Access
Temporary Records	Federal Records approved by NARA for disposal, either immediately or after a specified retention period.
Temporary Secure Working Area (TSWA)	Accredited Facilities where handling, discussing, or processing of SCI is limited to less than 40 hours per month and the Accreditation is limited to 12 months or less. Extension requests require a plan to accredit as an SCI Facility (SCIF) or Secure Working Area (SWA). SCI storage is not permitted within a TSWA.
Termination Briefing	***Synonym(s)***: Termination Security Briefing
Termination Security Briefing	A security briefing to remind individuals of their continued security responsibilities when their Access Authorization has been revoked, terminated, or suspended, which is recorded by the signing of a Debriefing Acknowledgement or through administrative action. ***Synonym(s)***: Termination Briefing; Debriefing; Security Debriefing; Read-Off

Terrorism Consequence Management	Preparations designed to negate, mitigate, or respond to the consequences of potential terrorists attacks including the use of Weapons of Mass Destruction (WMD).
Terrorism Threat Level	An intelligence Threat Assessment of the level of Risk associated with potential terrorist attack(s) on U.S. personnel and interests in a foreign country based on continuous intelligence analysis of five elements: terrorist group existence, capability, history, trends, and targeting. There are five Threat levels: Negligible, Low, Medium, High, and Critical. Threat levels should not be confused with DoD Terrorist Force Protection Conditions (FPCON), or Department of State Security Environment Threat List (SETL) assessments.
Terrorist Force Protection Condition (FPCON)	A DoD-approved system standardizing the identification of and recommended preventive actions and responses to terrorists Threats against U.S. personnel and Facilities. ***Synonym(s)*:** Terrorist Threat Condition; Force Protection Condition
Terrorist Incident Response Measures	A set of procedures in place for response forces to deal with the effects of a terrorist incident.
Terrorist Threat Condition (THREATCON)	This term in no longer in use. ***Synonym(s)*:** Terrorist Force Protection Condition
Tetragraph	A sequence of four letters used to represent an international organization, alliance, or other grouping of countries and international organizations.
Threat	The perceived imminence of intended aggression by a capable entity to harm a nation, a government or its instrumentalities, such as intelligence, programs, operations, people, installations, or facilities.
Threat Analysis	The analytic method used to assess the

	capabilities, intentions, and opportunity of an Adversary to exploit or damage Assets.
Threat Assessment	A component process of Risk Management that reviews the intentions and capabilities of potential Adversaries or Hazards, and their applicability to specific valued Assets; the product of such a review.
Tier 1 Investigation	A Personnel Security Investigation (PSI) conducted for positions designated as low risk, Non-Sensitive, and for Physical or Logical Access. ***Related Term(s)*:** Suitability; Credential; Investigative Tier Standards
Tier 2 Investigation	A Personnel Security Investigation (PSI) conducted for positions designated as moderate risk public trust. ***Related Term(s)*:** Suitability; Investigative Tier Standards
Tier 3 Investigation	A Personnel Security Investigation (PSI) conducted for positions designated as Non-Critical Sensitive, military Accessions, or requiring Eligibility for Access to "L," Confidential, or Secret information. This is the lowest level of investigation acceptable for Access to Classified Information. ***Related Term(s)*:** Eligibility; Investigative Tier Standards
Tier 4 Investigation	A Personnel Security Investigation (PSI) conducted for positions designated as high risk public trust. ***Related Term(s)*:** Suitability; Investigative Tier Standards
Tier 5 Investigation	A Personnel Security Investigation (PSI) conducted for positions designated as Critical-Sensitive or Special-Sensitive, or requiring Eligibility for Access to "Q," Top Secret (TS), or SCI. ***Related Term(s)*:** Eligibility; Investigative Tier Standards
Top Secret (TS)	See Classification Level.

Transclassification	Information that has been removed from the Restricted Data (RD) category in order to carry out provisions of the National Security Act of 1947, as amended, and safeguarded under applicable Executive Orders as National Security Information (NSI).
Trigraph	(1) A three-letter acronym for a classified Code Word. (2) A sequence of three letters used to represent a country. ***Synonym(s)*:** Country Code
Trusted Information Provider	An authorized individual working for or on behalf of the Federal Government, other than for the Investigation Service Provider (ISP), who corroborates Subject data, such as date and place of birth, citizenship, and education. These individuals may include Federal Government and Contractor Employees or military personnel working in human resources or security offices or in equivalent organizations. ***Related Term(s)*:** Personnel Security Investigation
Trusted Traveler	A procedure that allows for uniformed service members and spouses, DoD employees, and retired uniformed service members and spouses to vouch for occupants in their immediate vehicle, provided the Trusted Travelers are entirely responsible for the actions of all occupants in their vehicle for meeting all local security requirements for escort as established by installation authorities.
Two-Person Control	The continuous surveillance and control of positive control material by a minimum of two authorized individuals, each capable of detecting incorrect and unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements.
Two-Person Integrity (TPI)	A system of storage and handling designed to

	prohibit individual Access to certain COMSEC keying material by requiring the presence of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed.
Umbrella	A SAP may be referred to as an "umbrella" if the SAP has subordinate elements, referred as compartments, sub-compartments, or projects. ***Related Term(s)*:** Special Access Program
Unacceptable Risk	A Threat to the life, safety, or health of Employees, Contractors, vendors, or visitors; to the U.S. Government physical Assets or information systems; to personal property; to Records, including classified, privileged, proprietary, financial, and medical Records; or to the privacy rights established by The Privacy Act of 1974, as amended, or other law, that is deemed unacceptable when making Risk Management determinations.
Unacknowledged Special Access Program	A SAP having protective controls ensuring the existence of the program is not acknowledged, affirmed, or made known to any person not authorized for such information. ***Related Term(s)*:** Special Access Program
Unauthorized Disclosure	Communication or physical transfer of Classified or Controlled Unclassified Information (CUI) to an unauthorized recipient.
Uncaveated Information	Classified Information that carries no restrictive or permissive Control Markings.
Unclassified	Information that has not been determined to be Classified under Executive Order or statute.
Unescorted Individuals	Personnel who have been identity proofed and favorably vetted are eligible for unescorted access within the installation; but are,

	however, still subject to any controlled or restricted area limitations.
Unfavorable Adjudicative Determination	The final determination that results in a negative action relative to a person's Eligibility for Access to classified information, materials, or areas, or assignment to national security positions; or Suitability for employment, retention, or incumbency in a Sensitive or Public Trust Position; or issuance of a local, DoD, or federal credential; or authorization to Access a federally controlled space. ***Related Term(s)***: Due Process ***Synonym(s)***: Unfavorable Personnel Security Determination
Unfavorable Personnel Security Determination	***Synonym(s)***: Unfavorable Adjudicative Determination
United States Citizen	(1) A person born in the U.S. or any of its territories. (2) A person born abroad but having one or both parents who are themselves U.S. citizens. (3) A person who has met the requirements for citizenship as determined by Immigration and Customs Enforcement and has taken the requisite oath of allegiance. Note: United States Citizen is not a synonym of National of the United States. ***Related Term(s)***: Foreign National; United States National; Lawful Permanent Resident; United States Person
United States Entity	(1) State, Local, or Tribal governments. (2) State, Local, and Tribal law enforcement and firefighting entities. (3) Public health and medical entities. (4) Regional, State, Local, and Tribal emergency management entities, including State Adjutants General and other appropriate public safety entities. (5) Private sector entities serving as part of the U.S.'s Critical Infrastructure/Key Resources (CI/KR).

United States National	(1) A U.S. Citizen. (2) A non-U.S. Citizen whose only connection to the U.S. is through birth in an outlying possession (which as of 2005 is limited to American Samoa, Swains Island, and the unincorporated U.S. Minor Outlying Islands), or through descent from a person so born. ***Related Term(s)***: U.S. Citizen ***Synonym(s)***: National of the United States
United States Person	Any form of business enterprise or entity organized, chartered or incorporated under the laws of the U.S. or its territories; any person who is a U.S Citizen or National of the United States; and any person who is a Lawful Permanent Resident (LPR).
Upgrading	The determination that certain Classified Information requires, in the interests of National Security, a higher degree of protection against Unauthorized Disclosure than currently provided.
Variance	***Synonym(s)***: Technical Deviation
Vault	An area designed and constructed of masonry units or steel-lined construction to provide protection against forced entry and which is equipped with a GSA-approved Vault door and lock. A modular Vault approved by the GSA may be used in lieu of a Vault.
Vehicle Inspection	An inspection of a vehicle and contents for potentially harmful materials or devices.
Verify	The confirmation, by an independent and authoritative source, of the correctness and accuracy of information listed on the eApplication or provided by the Subject or other sources to the requesting agency or Investigative Service Provider (ISP). ***Related Term(s)***: eApplication
Veteran's Identification Card	A card issued by the U.S. Department of

(VIC)	Veterans Affairs (VA) used at VA medical Facilities for veterans to receive medical benefits. The card displays the veteran's name, picture, and any special eligibility indicators on the front of the card.
Vetting	***Synonym(s)*:** Screening
Violation	(1) Any knowing, willful, or negligent action that could reasonably be expected to result in an Unauthorized Disclosure of Classified Information. (2) Any knowing, willful, or negligent action to classify or continue the Classification of information contrary to Executive Order or implementing directive requirements. (3) Any knowing, willful, or negligent action to create or continue a SAP contrary to Executive Order requirements. ***Related Term(s)*:** Security Incident
Visit Authorization Request (VAR)	Temporary certification for Access to another organization or Facility to accomplish a task or to attend a meeting or seminar. ***Synonym(s)*:** Outgoing Visit Request
Visitor Control Center (VCC)	An Access Control Point at which visitors present themselves to gain Access to a Facility, Installation, building, or Restricted Area.
Vulnerability	A situation or circumstance, which left unchanged, may result in the loss of, or damage to, Assets.
Vulnerability Analysis	The analytic method used to assess the inherent susceptibility of a procedure, Facility, information system, equipment, or policy to an attack or exploitation.
Vulnerability Assessment	(1) A component process of Risk Management that reviews potential Vulnerabilities related to specific valued Assets that could be exploited by one or more Threats. (2) The product of such a review.
Waived Special Access Program	A SAP for which the Secretary of Defense

	has waived applicable reporting per statute (Section 119 of title 10, United States Code) following a determination of adverse effect to National Security. ***Related Term(s):*** Special Access Program
Waiver (Personnel Security)	See Exception.
Waiver (Physical Security)	*Synonym:* Exception.
Whole Person Concept	The model upon which an adjudicative authority makes a determination of an individual's Eligibility for Access to Classified Information or Suitability for a Public Trust Position. This concept involves the careful weighing of available information, favorable and unfavorable, both past and present, including mitigating factors.
Working Dog	Any canine bred, procured, or acquired to meet official requirements to support operations in the protection of Installations, Resources, and Personnel, to include explosive and illegal narcotic detection, patrol, tracking, or other security requirements. ***Synonym(s):*** Military Working Dog
Working Dog Handler	Trained dog handler partnered with a Working Dog as a team.
Working Paper or Materials	Material accumulated or created in the preparation of finished Documents or Records.
Write-For-Release	The practice of writing intelligence reports so as to disguise Intelligence Sources and Methods and thus enable distribution to customers or intelligence partners at lower Classification Levels. ***Related Term(s):*** Tearline Reporting