CDSE

Center for Development of Security Excellence

Industrial Security Comprehensive Glossary

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A	
Access	The ability and opportunity to gain knowledge of classified information.
Acquisition	The conceptualization, initiation, design, development, test, contracting, production, deployment, logistics support (LS), modification, and disposal of weapons and other systems, supplies, or services (including construction) to satisfy DOD needs intended for use in, or in support of, military missions.
Acquisition Life Cycle	The management process by which the DOD provides effective, affordable, and timely systems to the users. It consists of phases containing major activities and associated decision points during which a system goes through research, development, test, and evaluation (RDT&E); production; fielding or deployment; sustainment; and disposal. Currently, there are five phases, three milestone decisions, and four decision points.
Activity	Department of Defense (DOD) unit, organization, or installation performing a function or mission.
Activity Address Code (AAC)	The AAC is a distinct, six-position code consisting of a combination of alpha and/or numeric characters assigned to identify specific agency offices, units, activities, or organizations by the General Services Administration for civilian agencies and DOD for defense agencies.
Adjudication	The evaluation of personnel security investigations and other relevant information to determine if it is clearly consistent with the interests of national security for persons to be granted or retain eligibility for access to classified information and continue to hold positions requiring a trustworthy decision.
Adjudicator	A uniquely certified professional who is trained to assess an individual's loyalty, trustworthiness, and reliability, and determine whether it is in the best interest of national security to grant the individual an eligibility for access to classified information or render a favorable suitability determination.
Administrative Contracting Officer (ACO)	The ACO administers the day-to-day activities following the contract award. The ACO may not have official Contracting Officer status but may be a delegate of the Contracting Officer.
Adversary	An individual, group, organization, or government that must be denied Critical Program Information (CPI). Synonymous with competitor/enemy.
Adverse Information	Any information that adversely reflects on the integrity or character of a cleared employee and suggests that his

A	
	or her ability to safeguard classified information may be impaired, that his or her access to classified information may not be in the interest of national security, or that the individual constitutes an insider threat.
Affiliate	Each entity that directly or indirectly controls, is directly or indirectly controlled by, or is under common control with, the ultimate parent entity.
Agency	Any "Executive agency" as defined in Section 105 of Title 5, United States Code (U.S.C.), including the "military department," as defined in Section 102 of Title 5, U.S.C., and any other entity within the Executive Branch that releases classified information to private sector entities.
Alarm Service Company	An entity or branch office from which all installation, service, and maintenance of alarm systems are provided. The monitoring and investigation of such systems are either provided by the company's own personnel or with personnel assigned to this location.
Alien	A person who is not a citizen or national of the United States (8 U.S.C 1101(a)(3)). The term is synonymous with "foreign national."
Alternative Compensatory Control Measures (ACCM) Information	A head of a DOD Component with Original Classification Authority (OCA) may employ ACCM when he or she determines that the standard security measures detailed in the DODM 5200.01-V3 are insufficient to enforce need to know for classified information and Special Compartmented Information (SCI) or Special Access Programs (SAP) protections are not warranted. The use of an unclassified nickname, obtained in accordance with Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3150.29C (Reference (ae)), together with a list of persons authorized access, and a specific description of information subject to the enhanced ACCM controls, are the three requisite elements of an ACCM.
Anomaly	An activity or knowledge outside the norm that suggests a foreign entity has fore knowledge of U.S. information, processes, or capabilities.
Antiterrorism (AT)	Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include rapid containment by local military and civilian forces.
Applicant	A person other than an employee who has received an authorized conditional offer of employment for a position that requires access to classified information.
Approved Methods	Methods for repairing security containers that are obtained from the Cognizant Security Agency (CSA). A container that has been repaired using unapproved methods may no longer be used for storage of SECRET information even with supplemental controls.

A	
Approved Security Container	A Government Services Administration (GSA) approved security container originally procured through the Federal Supply system. The security containers bear the GSA Approval label on the front face of the container, which identifies them as meeting the testing requirements of the assigned federal specification and having been maintained according to Federal Standard 809.
Approved Vault	A vault built to Federal Standard 832 and approved by the CSA.
Arms, Ammunition and Explosives (AA&E) Program	This program provides guidance regarding the safety and security of arms, ammunition and explosives.
Articles of Incorporation	Serve as the legal means by which a company is incorporated. This document must be filed with the state and becomes part of the public record.
Assessment and Authorizations (A&A)	Approval for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and national security.
Assessment and Evaluation (A&E)	A&E monitors contractors for changes impacting their Facility Clearance (FCL) and performs data analysis, statistical reporting, and financial accuracy for Personnel Security Investigations (PSIs).
Assets	A person, structure, facility, information, material, or process that has value.
Atomic Energy Information	Information regarding nuclear weapons and special nuclear materials. Only the Department of Energy (DOE) may originally classify or declassify atomic energy information.
Authorized Person	A person who has a favorable determination of eligibility for access to classified information, has signed an approved non-disclosure agreement, and has a need-to-know.
Automatic Declassification	Declassification of information that is more than 25 years old and is not otherwise prevented from being declassified by an approved exemption. Such information shall be declassified on the 31st of December, 25 years from the date of original classification.

Back to Top

B	
Banner Markings	Indicates the highest level of classification of the overall document as determined by the highest level of any one portion within the document. They are placed on the top and bottom of every page of the document.
Bilateral Security Agreements	Collectively, the General Security Agreements and General Security of Information Agreements (GSOIAs), which pertain to the safeguarding of all classified information; the General Security of Military Information Agreements, which pertain to the safeguarding of

B	
	classified information generated by or for the DOD or which is under its jurisdiction or control; and the industrial security annexes to the General Security Agreements, GSOIAs, and General Security of Military Information Agreements.
Board Resolution (BR)	A legally binding document from the organization's governing board acknowledging the foreign investors and denying them access to classified or controlled information. Board Resolutions are adequate in cases where the foreign investor has a minority stake in the company, is not a member of the governing board, and has no right to appoint or elect a member of the board.
Branch Office	An office of an entity which is located somewhere other than the entity's main office location. A branch office is simply another location of the same legal business entity and is still involved in the business activities of the entity.
Business Structure	Organization framework legally recognized in a particular jurisdiction for conducting commercial activities such as sole proprietorship, partnership, and corporation.
By-laws	They establish how a company will conduct its business. By-laws are not generally filed with the state, nor are they part of the public record. The By-laws guide the officers in managing the company. They also describe the powers and authority of the company's directors and managers, and any limits on those powers.

Back to Top

C	
Center for Development of Security Excellence (CDSE)	A nationally accredited, award-winning directorate within the DCSA. The CDSE is the premier provider of security training, education, and certification for the DOD, Federal Government, and cleared contractors under the National Industrial Security Program (NISP)
Certificate Pertaining to Foreign Interest (SF 328)	A survey with questions designed to help identify the presence of Foreign Ownership, Control, or Influence (FOCI) in an organization, and provides the basis around which the FOCI analysis process is organized. The form is completed using the Facility Clearance (FCL) system of record.
Certification	A comprehensive evaluation of an information system component that establishes the extent to which a particular design and implementation meets a set of specified security requirements.
Citizen of the United States	All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the state wherein they reside. (Article14 of the U.S. Constitution) Individuals born in the United States, Puerto Rico, Guam, Northern Mariana

C	
	Islands, Virgin Islands, American Samoa, or Swain's Island; foreign-born children, children under age 18 residing in the United States with their birth or adoptive parents, at least one of whom is a U.S. citizen by birth or naturalization; and individuals granted citizenship status through naturalization by the Immigration and Naturalization Services are U.S. Citizens.
Classification	The determination that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made.
Classification Authority Block (CAB)	Indicates who the document was classified by, where it was derived from, downgrade instructions, and when it should be declassified. The CAB is placed on the face of each classified document near the bottom.
Classification Guide	A document issued by an authorized original classifier that identifies the elements of information regarding a specific subject that must be classified and prescribes the level and duration of classification and appropriate declassification instructions.
Classification Level	Classification levels are applied to National Security Information (NSI) that, if subject to unauthorized disclosure, could reasonably be expected to cause damage, serious damage, or exceptionally grave damage to national security. Each level has its own requirement for safeguarding information. The higher the level of classification, the more protection the classified information requires to reasonably prevent the possibility of its loss or compromise. Those levels, from lowest to highest, are CONFIDENTIAL, SECRET and TOP SECRET.
Classification Review	Review of compromised classified information to determine whether affected information should be declassified or downgraded and identify measures to keep it from becoming a threat to the Nation.
Classified Contract	Any contract requiring access to classified information by a contractor in the performance of the contract (a contract may be a classified contract even though the contract document is not classified). The requirements prescribed for a "classified contract" 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 Activity (GCA) program or project which requires access to classified information by a contractor.
Classified Critical Infrastructure Protection Program (CCIPP)	The secured sharing of classified information under a designated critical infrastructure protection program with authorized individuals and organizations as determined by the Secretary of Homeland Security.

C	
Classified Information	Information that has been determined pursuant to Executive Order (E.O.) 13526 or any predecessor order to require protection against unauthorized disclosure in the interest of national security. The term includes NSI, Restricted Data (RD), and Formerly Restricted Data (FRD).
Classified Information Non-Disclosure Agreement (NDA) (SF 312)	The SF 312 is an NDA between the U.S. Government and an individual who is cleared for access to classified information. An employee determined eligible for access to classified information must execute an NDA prior to being granted access to classified information.
Classified Information Spillage	Security incident that occurs whenever classified data is spilled either onto an unclassified information system, or to an information system with a lower level of classification or different security category.
Classified Meetings	A conference, seminar, symposium, exhibit, convention, training course, or other such gathering during which classified information is disclosed.
Classified Military Information (CMI)	Classified information that is under the control or jurisdiction of the Department of Defense, its departments, or agencies, or is of primary interest to them. It may be embodied in oral, visual, or other forms and requires protection in the interest of national defense and security in one of three classification categories – TOP SECRET, SECRET, or CONFIDENTIAL - as described in Executive Order 13526 or successor orders. It includes eight categories of information as described in the National Disclosure Policy (NDP-1).
Classified Visit	A visit during which a visitor will require, or is expected to require, access to classified information.
Classified Waste	Classified information that is no longer needed and is pending destruction.
Classified Working Papers	Documents that are generated in the preparation of a finished document.
Classifier	Any person who makes a classification determination and applies a classification category to information or material. The determination may be an original classification action or a derivative classification action. Contractors make derivative classification determinations based on classified source material, a security classification guide, or a contract security classification specification, or equivalent.
Clearance	Formal security determination by an authorized adjudicative office that an individual is authorized access, on a need-to-know basis, to a specific level of collateral classified information (TOP SECRET, SECRET, CONFIDENTIAL).

C	
Cleared Contractor (CC)	A person or facility operating under the National Industrial Security Program (NISP) that has had an administrative determination that they are eligible, from a security point of view, for access to classified information of a certain level and all lower levels.
Cleared Contractor Facility	Any industrial, educational, commercial facility, or other entity that has been granted a facility security clearance under the NISP.
Cleared Defense Contractor (CDC)	A subset of contractors cleared under the NISP who have contracts with the Department of Defense. Therefore, not all cleared contractors have contracts with DOD.
Cleared Employees	All industrial or commercial contractors, licensees, certificate holders, or grantees of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head who are granted Personnel Security Clearances (PCL) or are being processed for PCLs.
Closed Area	An area that meets the requirements of the NISPOM for safeguarding classified material that, because of its size, nature, or operational necessity, cannot be adequately protected by the normal safeguards or stored during non-working hours in approved containers.
Cognizant Security Agencies (CSAs)	Agencies of the Executive Branch that were authorized by Executive Order (EO) 12829 to establish an industrial security program to safeguard classified information under the jurisdiction of these agencies when disclosed or released to U.S. industry. Those agencies are: The Department of Defense (DOD), Office of the Director of National Intelligence (DNI), Department of Energy (DOE), and the Nuclear Regulatory Commission (NRC). EO 13691 established the Department of Homeland Security (DHS) as a CSA.
Cognizant Security Office (CSO)	The organizational entity delegated by the head of a Cognizant Security Agency (CSA) to administer industrial security on behalf of the CSA.
Commercial and Government Entity (CAGE) Code	A five-position code that identifies companies doing or wishing to do business with the Federal Government. The first and fifth positions in the code must be numeric. The third and fourth positions may be any mixture of alpha/numeric excluding I and O. The code is used to support a variety of mechanized systems throughout the Government.
Commercial Program	A program that is based on the initiative of a contractor with no U.S. Government involvement (e.g., direct commercial sales).
Committee on Foreign Investment in the United States (CFIUS)	An inter-agency committee authorized to review proposed mergers, acquisitions, or takeovers that could result in control of a U.S. business by a foreign interest in order to determine the effect of such transactions on the national security of the U.S.

C	
Common Access Card (CAC)	A CAC is a DOD smart card for multifactor authentication. CACs are issued as standard identification for active-duty military personnel, reserve personnel, civilian employees, non-DOD Government employees, state employees of the National Guard, and eligible contractor personnel.
Communications Security (COMSEC)	The protective measures taken to deny unauthorized persons information derived from United States Government telecommunications relating to national security and to ensure the authenticity of such communications.
Company	A generic and comprehensive term that 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.
Compilation	The concept also known as aggregation, which involves combining or associating individually unclassified information which reveals an additional association or relationship that warrants protection as classified information. This concept also applies to elements of information classified at a lower level which become classified at a higher level when combined.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Conclusion	A formal determination for each security violation. Define the security violation as a loss, compromise, suspected compromise, or no loss, compromise, or suspected compromise. Include vulnerability of information, description of unauthorized access, and description of GCA classification review.
CONFIDENTIAL	The classification level applied to information, the unauthorized disclosure of which could reasonably be expected to cause damage to the national security that the original classification authority (OCA) is able to identify or describe.
Consignee	A person, firm, or Government (i.e., United States Government or foreign government) activity named as the receiver of a shipment; one to whom a shipment is consigned.
Consignor	A person, firm, or Government (i.e., United States Government or foreign government) activity by which articles are shipped. The consignor is usually the shipper.
Constant Surveillance Service (CSS)	A transportation protective service provided by a commercial carrier qualified by the Surface Deployment and Distribution Command to transport CONFIDENTIAL

C	
	shipments. The service requires constant surveillance of the shipment at all times by a qualified carrier representative; however, an Facility Clearance (FCL) is not required for the carrier. The carrier providing the service must maintain a signature and tally record for the shipment.
Consultant	An individual under contract, and compensated directly, to provide professional or technical assistance to a contractor in a capacity requiring access to classified information.
Contained In	The concept that refers to the process of extracting classified information as it is stated in an authorized source of classification guidance without the need for additional interpretation or analysis and incorporating this information into a new document.
Continuous Evaluation	As defined in SEAD 6, a personnel security investigative process to review the background of a covered individual who has been determined to be eligible for access to classified information or to hold a sensitive position at any time during the period of eligibility. Continuous evaluation leverages a set of automated records checks and business rules to assist in the ongoing assessment of an individual's continued eligibility. It supplements, but does not replace, the established personnel security program for scheduled periodic reinvestigations of individuals for continuing eligibility.
Continuous Monitoring Program	A system that facilitates ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions.
Continuous Vetting (CV)	A real-time review of an individual's background at any time to determine if they continue to meet applicable eligibility requirements.
Contract Closeout	During this phase, the Contracting Officer must ensure that the work conforms to the requirements in the Statement of Work (SOW) or Performance Work Statement (PWS). Any deficiencies must be resolved before final payment is made. All classified material must be returned to the GCA or destroyed.
Contract Manager	Generally responsible for a company's contract management or the administration of contracts made with customers, vendors, partners, or employees. Contract management includes negotiating the terms and conditions in contracts and ensuring compliance, as well as documenting and agreeing on any changes or amendments that may arise during its implementation or execution.
Contracting Officer (CO)	A U.S. Government official who, in accordance with departmental or agency procedures, has the authority to enter into and administer contracts, licenses, or grants, and make determinations and findings with respect

C	
	thereto, or any part of such authority. The term also includes the designated representative of the contracting officer acting within the limits of his or her authority.
Contracting Officer's Representative (COR)	Determines the need for contractor access to classified information, verifies the Facility Security Clearance (FCL), and communicates the security requirements during the procurement process and contract performance to the contractor.
Contractor	Any industrial, educational, commercial, or other entity that has been granted an entity eligibility determination by a Cognizant Security Agency (CSA). This term also includes licensees, grantees, or certificate holders of the United States Government (USG) with an entity eligibility determination granted by a CSA. As used in the NISPOM, ''contractor'' does not refer to contractor employees or other personnel.
Control Markings	Identify the presence of special categories of classified information.
Controlled Unclassified Information (CUI)	Information the United States Government (USG) creates or possesses, or that an entity creates or possesses for or on behalf of the USG, that a law, regulation, or USG-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.
Cooperative Program	A program comprised of one or more specific cooperative projects with a foreign government or international organization whose arrangements are defined in a written agreement between the parties covering research, development, test, evaluation, and joint production, including follow-on support.
Cooperative Program Personnel (CPP)	Military or civilian employees of a foreign government or international organization who are assigned to a cooperative program at a DOD Component or DOD contractor facility.
Corporate Family	An entity, its parents, subsidiaries, divisions, and branch offices.
Corporation	A business owned by one or more legal entities. These entities can be individuals, partnerships, or even other corporations.
Corrective Actions	Any disciplinary actions taken against a culpable individual(s) involved in a security violation and the actions initiated or taken by the facility to secure the information after the violation.

C	
Counterintelligence (CI)	Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage or other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, persons, their agents, or international terrorist organizations.
Counterintelligence (CI) Special Agent (CISA)	Assists Facility Security Officers (FSOs) in identifying potential threats to U.S. technology and developing Counterintelligence (CI) awareness and reporting by company employees.
Countermeasure	The employment of devices or techniques that impair the operational effectiveness of enemy activity. Countermeasures may include anything that effectively negates an adversary's ability to exploit vulnerabilities.
Courier	A cleared employee designated by the contractor whose principal duty is to transmit classified material to its destination, ensuring that the classified material remains under their constant and continuous protection, and that they make direct point-to-point delivery.
Critical Nuclear Weapon Design Information (CNWDI)	A Department of Defense (DOD) category of TOP SECRET Restricted Data (RD) or SECRET Restricted Data (RD) that reveals the theory of operation or design of the components of a thermonuclear or fission bomb, warhead, demolition munition, or test device.
Critical Program Information (CPI)	Elements or components of a research, development, and acquisition (RDA) program 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.
Critical-sensitive	Any civilian national security position that has the potential to cause exceptionally grave damage to national security.
Critical Technology	Technology or technologies essential to the design, development, production, operation, application, or maintenance of an article or service that makes or could make a significant contribution to the military potential of any country, including the U.S.
CRYPTO	The marking or designator that identifies unencrypted COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive United States Government (USG) or USG-derived information. This includes non-split keying material used to encrypt or decrypt COMSEC critical software and software-based algorithms.
Cryptographic Device	A device or piece of equipment which uses cryptographic logic to protect information by converting plain text to cipher text and vice versa.

C	
Custodian	An individual who has possession of, or is otherwise charged with, the responsibility for safeguarding classified information.
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
Cyber Incident	Actions taken using computer networks that result in an actual or potentially adverse effect on an information system or the information residing therein.

Back to Top

D	
Damage Assessment	A determination of the effect of a compromise of classified information on national security.
Data Spill	Known also as contaminations or classified message incidents, occurs when classified data or controlled unclassified information (CUI) is introduced to an unclassified computer system or to a computer system accredited at a lower classification level than the data being entered.
Debriefing	The process of informing a person their need-to-know for access is terminated.
Declassification	A date or event that coincides with the lapse of the information's national security sensitivity as determined by the original classification authority (OCA). Declassification occurs when the OCA determines that the classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure, and the information has had its classification designation removed or cancelled.
Defense Articles	Those articles, services, and related technical data, including software, in tangible or intangible form, which are listed on the United States Munitions List (USML) of the International Traffic in Arms Regulations (ITAR), as modified or amended. Defense articles exempt from the scope of ITAR section 126.17 are identified in Supplement No. 1 to Part 126 of the ITAR.
Defense Central Index of Investigations (DCII)	An automated DOD repository that identifies investigations conducted by DOD investigative agencies and personnel security determinations made by DOD adjudicative authorities.
Defense Counterintelligence and Security Agency (DCSA)	An agency of the DOD located in Quantico, Virginia. The Under Secretary of Defense for Intelligence and Security provides authority, direction, and control over DCSA. DCSA supports national security and the service

D	
	members, secures the nation's technological base, and oversees the protection of U.S. and foreign classified information in the hands of industry. DCSA accomplishes this mission by clearing industrial facilities, accrediting information systems, facilitating the personnel security clearance process, delivering security education, training, and certification, and providing information technology services that support the industrial and personnel security missions of DOD and its partner agencies.
Defense Counterintelligence and Security Agency (DCSA), Counterintelligence Special Agent (CISA)	Assists FSOs in identifying potential threats to U.S. technology and developing CI awareness and reporting by company employees.
Defense Counterintelligence and Security Agency (DCSA), Field Office Chief (FOC)	Manages the implementation of NISP and AA&E programs. Ensures effective counterintelligence support to cleared facilities and Government contracting activities throughout the area of responsibility. Oversees the conduct of security reviews by IS Reps. Manages office budget, vehicle utilization, and other property.
Defense Counterintelligence and Security Agency (DCSA), Industrial Security Representative (IS Rep)	Local representative from the DCSA that provides advice and assistance to establish the security program and to ensure a facility is in compliance with the NISP.
Defense Counterintelligence and Security Agency (DCSA), Information Systems Security Professional/Security Control Assessor (ISSP/SCA)	Performs oversight of a contractor's information system processing classified information and provides an authorization decision recommendation to the Authorizing Official (AO).
Defense Counterintelligence and Security Agency (DCSA), National Industrial Security Program Authorization Office (NAO)	Office within the DCSA that facilitates the Assessment and Authorization (A&A) process for classified information systems at cleared contractor facilities.
Defense Courier Service (DCS)	A system that provides for the secure and expeditious transportation and delivery of qualified material which requires controlled handling by courier. DCS is the primary means of transferring SCI documents.
Defense Federal Acquisition Regulation Supplement (DFARS)	Implements and supplements the Federal Acquisition Regulation (FAR), and is administered by the Department of Defense (DOD). The DFARS should be read in conjunction with the primary set of rules in the FAR.
Defense Industrial Base (DIB)	The Department of Defense, government, and private sector worldwide industrial complex with capabilities to perform research and development and design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements.
Defense Information System for Security (DISS)	The enterprise case management system for national security, suitability, and credentialing eligibility mission areas. DISS replaced the Joint Personnel Adjudication System (JPAS) as the System of Record on March 31, 2021. An integral step toward the National Background Investigation Services (NBIS), it consists of three main components, the Case Adjudication Tracking System (CATS), the Joint Verification System, and Appeals.

D	
Defense Office of Hearing and Appeals (DOHA)	Provides hearings and issues decisions in PCL cases for contractor personnel doing classified work for all DOD Components and other Federal Agencies and Departments. If the DOD Consolidated Adjudications Facility (DOD CAF) cannot favorably find that it is clearly consistent with the national interest to make a final eligibility determination, the case is referred to DOHA for further processing and/or where the case will be decided before an Administrative Judge.
Defense Service	1. The furnishing of assistance (including training) to foreign persons, whether in the United States or abroad, in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles. 2. The furnishing to foreign persons of any technical data controlled, whether in the United States or abroad. 3. Military training of foreign units and forces, regular and irregular, including formal or informal instruction of foreign persons in the United States or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise, and military advice.
Defense Technical Information Center (DTIC)	The repository for research and engineering information for the Department of Defense (DOD). Its Suite of Services is available to DOD personnel, defense contractors, Federal Government personnel, contractors, and selected academic institutions. The general public can also access unclassified, unlimited information, including many full-text downloadable documents, through the public DTIC web site.
Defense Visit Office (DVO)	The Offices established by the Departments of the Army (Army Foreign Disclosure Office, DAMI-CD), Navy (Navy International Programs Office, NIPO-01D2), Air Force (Air Force Deputy Under Secretary of the Air Force for International Affairs, (SAF/IA), and DIA (Defense Foreign Liaison Office) to receive, coordinate, and respond to a Request for Visit (RFV). The Military Departments process the requests for their organizations and contractors. The DIA processes the requests for its organizations, as well as the Office of the Secretary of Defense, the Joint Staff, and the Defense Agencies.
Department of Defense (DOD)	The largest of five CSAs, having issued the most classified contracts to industry. Additionally, the Secretary of Defense has entered into agreements with other federal agencies for the purpose of rendering industrial security services.

D	
Department of Defense (DOD) Consolidated Adjudications Facility (DOD CAF)	The DOD CAF is the sole authority to determine security clearance eligibility of Non-Intelligence agency DOD personnel occupying sensitive positions and/or requiring access to classified material, including Sensitive Compartmented Information (SCI). The DOD CAF determines a final eligibility in accordance with the ODNI SEAD 4, National Security Adjudicative Guidelines, based on review and consideration from results and other available, reliable information collected from the national security background investigation.
Department of Defense Contract Security Classification Specification (DD Form 254)	This document provides security guidance to both the contractor and the Government. It is a legal document that directs the contractor about the proper protection of classified material released under the contract.
Department of Defense Security Agreement (DD Form 441)	A DOD Security Agreement between a contractor who will have access to classified information and the DOD in order to preserve and maintain the security of the U.S. through the prevention of unauthorized disclosure of classified information.
Department of Defense Security Agreement Appendage (DD Form 441-1)	The appendage to the DOD Security Agreement and lists—if applicable—cleared divisions or branches included in and covered by the provisions of the organization's DOD Security Agreement (DD Form 441) and Certificate Pertaining to Foreign Interest (SF 328).
Department of Defense (DOD) Security System of Record	A system of record for personnel security, adjudication determination, clearance, verification, and history. The term applies not only to this system, but to any successor of the DOD personnel security system of record.
Derivative Classification	The incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes classifying information based on classification guidance. Duplicating or reproducing existing classified information is not derivative classification.
Designated Disclosure Authority (DDA)	A military or civilian government official designated by the Head of a DOD Component or by the DOD Component's Principal Disclosure Authority (PDA), who has been delegated disclosure authority to control disclosures of Classified Military Information (CMI) and Controlled Unclassified Information (CUI) to foreign governments or international organizations and their representatives.
Designated Government Representative (DGR)	An individual serving as a DOD or other United States Government transmittal authority overseeing the transfer of classified defense articles and technical data through official government-to-government channels, or through other channels agreed upon by both governments.

D	
Destruction	Destroying classified information so that it can't be recognized or reconstructed.
Direct Commercial Sales (DCS)	A direct contractual arrangement between a commercial company and a foreign government, or international organization, or another commercial company.
Dissemination Controls	Identify the expansion or limitation on the distribution of information.
Document	Any recorded information, regardless of the nature of the medium, or the method or circumstances of recording.
Downgrade	A determination by a declassification authority that information classified and safeguarded at a specified level will be classified and safeguarded at a lower level.
Dual-use	Technology and articles that are potentially used either for commercial/civilian purposes or for military, defense, or defense-related purposes.
Duration	A determination made regarding how long information is to be protected (i.e., when the information will lose its sensitivity and no longer merit or qualify for classification).
Duties (for National Security)	Duties performed by individuals working for, or on behalf of, the Federal Government that are concerned with the protection of the U.S. from foreign aggression or espionage. This includes development of defense plans or policies, intelligence or counterintelligence (CI) activities, and related activities concerned with the preservation of the military strength of the U.S including duties that require eligibility for access to classified information in accordance with E.O. 12968.

Back to Top

E	
Electronic Communications Plan (ECP)	Puts policies and procedures regarding effective oversight of communications into place. This includes all media such as telephones, teleconferences, video conferences, facsimiles, cell phones, PDAs, and all other computer communication, including emails and server access. It applies to communications between contractor personnel, the foreign parent and affiliates, and subsidiaries. The ECP deters and detects influence by the foreign owner and unauthorized attempts to gain access to classified or controlled information.
Electronic Processing	The capture, storage, manipulation, reproduction, or transmission of data in all forms by any electronically-powered device. This definition includes, but is not limited to, computers and their peripheral equipment, word processors, office equipment, telecommunications equipment, facsimiles, and electronic accounting machines, etc.

E	
Elicitation	In intelligence usage, the acquisition of information from a person or group in a manner that does not disclose the intent of the interview or conversation.
Eligibility	The DOD Consolidated Adjudications Facility (DOD CAF) has made an adjudicative determination of a person's Personnel Security Investigation (PSI). That person will have access to classified information equal to the level of their adjudicated investigation.
Eligibility Determination	The decision to grant eligibility for access to classified information or performance of national security duties.
Embedded System	An information system (IS) that performs or controls a function, either in whole or in part, as an integral element of a larger system or subsystem such as ground support equipment, flight simulators, engine test stands, or fire control systems.
Employee	A person, other than the President and Vice President of the U.S., employed by, detailed, or assigned to an agency, including members of the Armed Forces. An expert or consultant to an agency, an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors, a personal services contractor, or any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head.
Empowered Official	A person at a U.S. company who is empowered to sign export authorizations or other international-related documents. The Empowered Official has authority to inquire into any aspect of an export or import, verify the legality of the transaction, and refuse to sign any application or other request without prejudice or other adverse recourse.
Entity	A generic and comprehensive term which may include sole proprietorships, partnerships, corporations, limited liability companies, societies, associations, institutions, contractors, licensees, grantees, certificate holders, and other organizations usually established and operating to carry out a commercial, industrial, educational, or other legitimate business, enterprise, or undertaking, or parts of these organizations. It may reference an entire organization, a prime contractor, parent organization, a branch or division, another type of sub-element, a sub-contractor, subsidiary, or other subordinate or connected entity (referred to as ''sub-entities'' when necessary to distinguish such entities from prime or parent entities). It may also reference a specific location or facility, or the headquarters or official business location of the organization, depending upon the organization's business structure, the access needs involved, and the responsible Cognizant Security Agency's (CSA) procedures. The term ''entity'' as

E	
	used in the 32 CFR Part 117 Rule refers to the particular entity to which an agency might release, or is releasing, classified information, whether that entity is a parent or subordinate organization. The term "entity" in this rule includes contractors.
Entity Eligibility Determination	An assessment by the CSA as to whether an entity is eligible for access to classified information of a certain level (and all lower levels). Entity eligibility determinations may be broad or limited to specific contracts, sponsoring agencies, or circumstances. A favorable entity eligibility determination results in eligibility to access classified information under the cognizance of the responsible CSA to the level approved. When the entity would be accessing categories of information such as RD or SCI for which the CSA for that information has set additional requirements, CSAs must also assess whether the entity is eligible for access to that category of information. Some CSAs refer to their favorable entity eligibility determinations as FCLs. However, a favorable entity eligibility determination for the DHS CCIPP is not equivalent to an FCL and does not meet the requirements for FCL reciprocity. A favorable entity eligibility determination does not convey authority to store classified information.
Escort	A cleared person designated by the contractor who accompanies a shipment of classified material to its destination. The classified material does not remain in the personal possession of the escort, but the conveyance in which the material is transported remains under the constant observation and control of the escort.
Espionage	Espionage is a national security crime; specifically, it violates Title 18 USC, §§ 792-798 and Article 106a, Uniform Code of Military Justice (UCMJ). Espionage convictions require the transmittal of national defense information with intent to aid a foreign power or harm the U.S. However, even gathering, collecting, or losing national defense information can be prosecuted under Title 18.
Espionage Indicators	Warning signs that an insider may be working for, or is susceptible to, control by a Foreign Intelligence Entity (FIE). These warning signs are the result of an insider's actions, activities, and behaviors that may be indicative of potential espionage-related activity.
Essential Facts	Provide description of the circumstances surrounding the violation, the relevant sections of the NISPOM that were violated, who was involved, and when and where the violation occurred. Include the level and type of personnel clearance of the individuals involved in the occurrence.

E	
Exception	An adjudicative decision to grant initial or continued eligibility for access to classified information or to hold a sensitive position despite failure to meet the full adjudicative or investigative standards.
Excluded	A determination by the CSA that Key Management Personnel (KMP) can be formally excluded from classified access. The applicable KMP will affirm as appropriate and provide a copy of the exclusion action to the CSA. This action will be made a matter of record by the organization's governing body.
Excluded Parties List System (EPLS)	Electronic directory of individuals and organizations that are not permitted to receive federal contracts or assistance from the United States Government.
Exclusion Resolution	An exclusion action record with language affirming that applicable KMP will not require, will not have, and can be effectively and formally excluded from, access to all classified information disclosed to the company and does not occupy a position that would enable them to adversely affect the organization's policies or practices in the performance of classified contracts.
Executive Order (E.O.)	An order issued by the President of the U.S. to create a policy and regulate its administration within the Executive Branch.
Executive Order (E.O.) 13526	Establishes the legal authority for certain officials within the Executive Branch of the Federal Government to designate classified national security information.
Export	Sending or taking a defense article out of the U.S. in any manner, except by mere travel outside of the U.S.by a person whose personal knowledge includes technical data; or 1. Transferring registration, control, or ownership to a foreign person of any aircraft, vessel, or satellite covered by the U.S. Munitions List, whether in the United States or abroad. 2. Disclosing (including oral or visual disclosure) or transferring any defense article to an embassy, agency, or subdivision of a foreign government (e.g., diplomatic missions) while in the U.S. 3. Disclosing (including oral or visual disclosure) or transferring technical data to a foreign person whether in the United States or abroad. 4. Performing a defense service on behalf of, or for the benefit of, a foreign person whether in the United States or abroad. 5. A launch vehicle or payload shall not, by reason of the launching of such vehicle, be considered an export for the purposes of this definition. However, for certain limited purposes, the controls of this definition may apply to any sale, transfer, or proposal to sell or transfer defense articles or defense services.

E	
Export Administration Regulations (EAR)	The U.S. Department of Commerce administers the EAR (15 CFR §730-774), which regulate the export of "dual-use" items. These items include goods and related technology, including technical data and technical assistance, which are designed for commercial purposes, but which could have military applications, such as computers, aircraft, and pathogens.
Export Authorization	An approved numbered license or agreement, or an authorized exemption under the International Traffic in Arms Regulation (ITAR).
Extent of Protection	The designation (such as ''Complete'') used to describe the degree of alarm protection installed in an alarmed area.
Extended Visit Authorization	Permits a single visit for an extended period of time. Extended visit authorizations are to be used when a foreign national is to be assigned to a Department of Defense (DOD) Component or a DOD contractor facility.
Extracting	Taking information directly from an authorized source of classification guidance and stating it verbatim in a new or different document.

Back to Top

F	
Facility	A plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components that, when related by function and location, form an operating entity.
Facility (Security) Clearance (FCL)	An administrative determination that, from a security viewpoint, an entity is eligible for access to classified information of a certain level (and all lower levels).
FCL Sponsorship	A request for a company FCL when a definite classified procurement need to access classified information is established. A company must be sponsored by either a company currently cleared to participate in the NISP or a GCA.
Facility Security Officer (FSO)	A U.S. citizen employee appointed by a contractor who will supervise and direct security measures necessary for implementing the NISPOM and other Federal requirements for classified information.
Federal Acquisition Regulation (FAR)	Contains the rules for Government acquisition. These rules provide instruction, forms, and guidance on Government contracting.
Federal Acquisition Regulation (FAR) Clause	Applies to the extent that the contract involves access to information classified as CONFIDENTIAL, SECRET, or TOP SECRET. The clause further states that the contractor shall comply with the Security Agreement (DD Form 441, including the National Industrial Security Program Operating Manual (NISPOM) and any revisions

F	
	to the manual, notice of which has been furnished to the contractor.
Federal Investigative Standards (FIS)	Standards that apply to investigations that determine eligibility for access to classified information, for holding a national security position, for physical and logical access, and for suitability for Government employment. The revised FIS, dated December 2012, established a new investigative model, which aligns and standardizes national security background investigation requirements for Homeland Security Presidential Directive 12 (HSPD-12), suitability and fitness, and national security into five tiers. The five-tiered model facilitates reciprocity, uses a build-upon (but not duplicate) investigative principle, and facilitates the use of automation to improve cost, quality, and timeliness of background investigations.
Final Report	Upon completion of a security violation investigation, the contractor must submit a final report to DCSA regarding the identified security violation. The final report builds upon the Initial Report and presents a summary of the investigation.
Foreign Government Information (FGI)	Information that is: provided to the U.S. by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or produced by the U.S. pursuant to, or as a result of, a joint arrangement with a foreign government or governments, an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence.
Foreign Interest	Any foreign government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized, chartered, or incorporated under the laws of any country other than the U.S. or its territories, and any person who is not a citizen or national of the U.S.
Foreign Investment	A company or individual from one nation invests in assets or ownership stakes of a company based in another nation.
Foreign Military Sales (FMS)	That portion of U.S. security assistance for sales programs that require agreements/contracts between the U.S. Government and an authorized recipient government or international organization for defense articles and services to be provided to the recipient for current stocks or new procurements under DOD-managed contracts, regardless of the source of financing.
Foreign National	Any person who is not a citizen or national of the U.S.
Foreign Ownership, Control or Influence (FOCI)	A U.S. company is considered to be under FOCI whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not

F	
	exercisable through the 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 adversely affect the performance of classified contracts.
Foreign Ownership, Control or Influence (FOCI) Action Plan	A method applied to negate or mitigate risk of foreign ownership or control. Also referred to as a mitigation instrument. Includes the Board Resolution, Security Control Agreement, Special Security Agreement, Proxy Agreement, and Voting Trust Agreement.
Foreign Ownership, Control or Influence (FOCI) Mitigation	The instruments and agreements put in place to reduce the effect of FOCI on a company's management decisions, and thus reducing the risk of unauthorized access to classified information.
Foreign Ownership, Control or Influence (FOCI) Signatory Company	The legal entity that signed the FOCI Mitigation Instrument, typically the corporate or home office.
Foreign Person	Any natural person who is not a lawful permanent resident as defined by 8 United States Code (U.S.C.) 1101(a)(20) or who is not a protected individual as defined by 8 U.S.C. 1324b(a)(3). It also means any foreign corporation, business association, partnership, trust, society or any other entity or group that is not incorporated or organized to do business in the United States, as well as international organizations, foreign governments, and any agency or subdivision of foreign governments (e.g., diplomatic missions).
Foreign Representative	A foreign national or any other person who represents or is sponsored by a foreign government or international organization.
Foreign Visit	A foreign national enters or proposes to enter a DOD Component or cleared contractor facility or to meet with employees or representatives of the facility.
Foreign Visit System (FVS)	The automated system that provides staffing and database support for processing RFVs by representatives of foreign governments and/or international organizations to DOD Component activities and defense contractors. The FVS is a controlled access system, which is accessed through the Secure Internet Protocol Router Network (SIPRNet).
Form DSP-5	Application/License for permanent export of unclassified defense articles and related technical data.
Form DSP-83	Non-transfer and use certificate.
Form DSP-85	Application/license for permanent/temporary export or temporary import of classified defense articles and related classified technical data.
Form DSP-94	Authority to export Defense articles and Defense services sold under the Foreign Military Sales program. The export authorization is comprised of the Form DSP-94 and a copy of the Letter of Offer and Acceptance.

F	
Formerly Restricted Data (FRD)	Classified information removed from the Restricted Data category upon a joint determination by the Department of Energy (DOE) and DOD that such information relates primarily to the military utilization of atomic weapons and that such information can be adequately safeguarded as classified defense information.
Freedom of Information Act (FOIA)	A provision that any person has a right, enforceable in court, of access to federal agency records, except to the extent that such records, or portions thereof, are protected from disclosure by one of nine exemptions.
Freight Forwarder (Transportation Agent)	Any agent or facility designated to receive, process, and transship U.S. material to foreign recipients. In the context of the NISPOM, it means an agent or facility cleared specifically to perform these functions for the transfer of U.S. classified material to foreign recipients.

Back to Top

G	
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 as General Security of Information Agreements, while others are limited to classified military information and are referred to as General Security of Military Information Agreements.
Generating	Taking information from an authorized source of classification guidance and using it in another form or media.
Government Contracting Activity (GCA)	An element of an agency that the agency head has designated and delegated broad authority regarding acquisition functions. A foreign government may also be a GCA.
Government Information (Official)	A step in the original classification process; for information to be identified as official, it must be owned by, produced by or for, or under the control of the U.S. Government.
Government-Owned Contractor Operated (GOCO)	A manufacturing plant that is owned by the Government and operated by a civilian organization under contract to the Government.
Government Program	A program that is initiated by a DOD Component (e.g., a program properly documented by an FMS Letter of Offer and Acceptance (LOA), a cooperative program

G	
	international agreement, combined military operations and training, or U.S. military operations).
Government Security Committee (GSC)	A permanent subcommittee of the board of directors made up of the Outside Director(s), Proxy Holders, or Voting Trustees, and any directors that hold personnel security clearances.
Government-to-Government Channels	The Defense Transportation System, the Defense Courier Service, the Military Postal Service Registered Mail, the Diplomatic Pouch Service, or other U.S. Government agency services which maintains constant U.S. Government control of the material being transferred; equivalent services provided by a foreign government or international organization.
Government-to-Government Transfer	Transfers through government-to-government channels or through other channels that the sending and receiving governments have agreed to in writing. In the latter case, the procedures must provide for accountability and control from the point of origin to the ultimate destination.
Grant	A legal instrument which, consistent with 31 United States Code (U.S.C.) 6304, is used to enter into a relationship: (a) Of which the principal purpose is to transfer a thing of value to the recipient to carry out a public purpose of support or stimulation authorized by a law of the United States, rather than to acquire property or services for the United States Government's (USG) direct benefit or use; or, (b) In which substantial involvement is not expected between DOD and the recipient when carrying out the activity contemplated by the award. The term grant may include both the grant and cooperative agreement.
Grantee	The entity that receives a grant or cooperative agreement.

Back to Top

H	
Hand Carrier	A cleared employee, designated by the contractor, who occasionally hand carries classified material to its destination in connection with a classified visit or meeting. The classified material remains in the personal possession of the hand carrier except for authorized overnight storage.
Home Office	The headquarters of a multiple-facility entity.
Human Intelligence (HUMINT)	Intelligence derived from information collected and provided by human sources.

Back to Top

I	
Imagery Intelligence (IMINT)	Uses satellite imagery, photographs, and other images to collect information.

I	
Impact	A step in the original classification process that assesses the probable operational, technological, and resources of classification.
Inadvertent Exposure	A set of circumstances or a security incident in which a person has had involuntary access to classified information that he or she was or is not normally authorized.
Individual Culpability	An individual responsible for a security violation plus evidence of deliberate disregard, gross negligence, and a pattern of negligence or carelessness.
Industrial Espionage	The knowing misappropriation of trade secrets related to, or included in, a product that is made for, or placed in, interstate or foreign commerce to the economic benefit of anyone other than the owner, with the knowledge or intent that the offense will injure the owner of that trade secret.
Industrial Security	That portion of information security concerned with the protection of classified information in the custody of U.S. industry.
Industrial Security Letter (ISL)	Documents that provide detailed operational guidance and notification of changes to, or clarification of, existing policies or requirements to the National Industrial Security Program Operating Manual (NISPOM).
Industrial Security Representative (IS Rep)	Local representative from the DCSA that provides advice and assistance to establish the security program and to ensure a facility is in compliance with the National Industrial Security Program (NISP).
Information	Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics.
Information Management System (IMS)	A system to protect and control classified information as required by NISPOM. The IMS must be capable of facilitating retrieval and disposition of classified material in a reasonable period of time.
Information Security	The system of policies, procedures, and requirements established pursuant to executive order, statute, or regulation to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security. The term also applies to policies, procedures, and requirements established to protect unclassified information that may be withheld from release to the public.
Information Security Oversight Office (ISOO)	Office responsible for implementing and monitoring the National Industrial Security Program (NISP) and for issuing and implementing directives that shall be binding on agencies.
Information System	An assembly of computer hardware, software, and firmware configured for the purpose of automating the functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating, or

I	
	otherwise manipulating data, information, and textual material.
Information System Security Manager (ISSM)	An individual appointed by a contractor with oversight responsibility for the development, implementation, and evaluation of the facility's classified information system security program. The ISSM must be trained to a level commensurate with the complexity of the facility's information system.
Information System Security Officer (ISSO)	Assigned by the Information System Security Manager (ISSM) when the facility has multiple authorized Information Systems (IS) in multiple facility organizations in which the ISSM has oversight responsibility for the multiple facilities, or when the technical complexity of the facility's IS program warrants the appointment.
Information System Security Professional /Security Control Assessor (ISSP/SCA)	An employee of DCSA that performs oversight of a contractor's information system processing classified information and provides an authorization decision recommendation to the Authorizing Official (AO).
Initial Report	When a security violation has occurred, the contractor will submit an initial report to DCSA to effectively and quickly communicate basic information related to the violation.
Inside Director	The representative appointed by the foreign interest (directly or indirectly) to serve on the Board of an SSA or SCA company. These individuals are formally excluded from access to classified information and their participation in the management of the company is limited to the extent allowed by the mitigation agreement.
Insider	Cleared contractor personnel with authorized access to any United States Government (USG) or contractor resource, including personnel, facilities, information, equipment, networks, and systems.
Insider Threat	The likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to contractor or program information to the extent that the information affects the contractor or agency's obligations to protect classified national security information.
Insider Threat Program Senior Official (ITPSO)	A U.S. citizen employee of the contractor who is cleared as part of the Facility Clearance (FCL). The ITPSO is responsible for establishing and executing the facility's insider threat program.
Intelligence	The product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information that concerns one or more aspects of foreign nations or of areas of foreign operations, and that is immediately or potentially significant to military planning and operations.

I	
Intelligence Community (IC)	Elements or any other department or agency as may be designated by the U.S. President or designated jointly by the ODNI and the head of the department or agency concerned, as an element of the IC, and as defined by the National Act of 1947, as amended, or by a successor order.
Interim FCL Determination	An interim FCL, also referred to as an entity eligibility determination, made on a temporary basis pending completion of the full investigative requirements. If results are favorable, following completion of full investigative requirements, the interim eligibility for access to classified information will become final. When a contractor with an interim FCL determination is unable or unwilling to comply with the requirements of the NISPOM and CSA-provided guidance regarding the process to obtain a final FCL, the CSA will withdraw the interim FCL.
Interim Personnel (Security) Clearance (PCL):	An interim PCL, or eligibility for access to classified information, as appropriate, is granted to an individual on a temporary basis, pending completion of the full investigative requirements, provided there is no evidence of adverse information that calls into question an individual's eligibility for access to classified information. If results are favorable following completion of full investigative requirements, the interim eligibility for access to classified information will become final. When an interim PCL determination has been made and derogatory information is subsequently developed, the CSA may withdraw the interim PCL.
International Agreement (IA)	An agreement concluded with one or more foreign governments (including their agencies, instrumentalities, or political subdivisions) or with an international organization, that: 1. Is signed or agreed to by personnel of a Department or Agency of the U.S. Government. 2. Signifies the intention of its parties to be bound in international law. 3. Is denominated as an international agreement or as a memorandum of understanding, memorandum of agreement, memorandum of arrangements, exchange of notes, exchange of letters, technical arrangement, protocol, note verbal, aide memoire, agreed minute, contract, arrangement, statement of intent, letter of intent, statement of understanding, or any other name connoting a similar legal consequence. The following are not considered international agreements: 1. Contracts made under the Federal Acquisition Regulations (FAR). 2. Foreign Military Sales Credit Agreements,

I	
	3. Foreign Military Sales Letters of Offer and Acceptance and Letters of Intent, (iv) Standardization Agreements, (v) Leases under 10 U.S.C. 2667, 2675 and 22 U.S.C. 2796. 4. Agreements solely to establish administrative procedures. 5. Acquisitions or orders that follow cross-servicing agreements made under the authority of the North Atlantic Treaty Organization (NATO) Mutual Support Act.
International Program	A lawful and authorized government or commercial effort in which there is a contributing or receiving foreign participant and information or technology is transferred from one country to another.
International Traffic in Arms Regulations (ITAR)	Implements the provisions of the Arms Export Control Act (AECA) and controls the export and import of defense-related articles and services on the U.S. Munitions List.
International Transfer	The transfer of material to a foreign government or international organization or their duly appointed representative in the United States, in the intended recipient country, or in a third country.
International Visit Program (IVP)	Used to process visits and assignments of foreign nationals to the DOD Components and cleared contractor facilities. IVP is designed to ensure that classified information and CUI to be disclosed to visitors has been properly authorized for disclosure to their governments, to ensure that the requesting foreign government provides a Security Assurance for the proposed visitor when classified information is involved in the visit or assignment, and to facilitate administrative arrangements (e.g., date, time, and place) for the visit or assignment.
Intrusion Detection System (IDS)	A security system that is designed to detect a change in the environment and transmit some type of alarm notification.
Invalidation	An administrative action that renders a contractor ineligible to receive or access additional classified material except that information necessary for completion of essential contracts as determined by appropriate Government Contracting Activity (GCA).
Investigation	The action of investigating something or someone; formal or systematic examination or research.
Investigative Service Provider (ISP)	A federal agency or federal contract agency that conducts National Security Background Investigations for the DOD.
Invitation For Bid (IFB):	A call to contractors to submit a proposal on a project for a specific product or service.

Back to Top

J	
Joint Venture (JV)	An association of two or more persons or entities engaged in a single defined project with all parties contributing assets and efforts and sharing in the management, profits, and losses in accordance with the terms of an agreement among the parties.
Joint Worldwide Intelligence Communications System (JWICS)	A TOP SECRET/SCI network run by the U. S. Defense Intelligence Agency and used across the DOD, Department of State, Department of Homeland Security, and Department of Justice to transmit especially sensitive classified information.

Back to Top

K	
Key Management Personnel (KMP)	An entity's Senior Management Official (SMO), Facility Security Officer (FSO), Insider Threat Program Senior Official (ITPSO), and all other entity officials who either hold majority interest or stock in, or have direct or indirect authority to, influence or decide issues affecting the management or operations of the entity or classified contract performance.

Back to Top

L	
L Access Authorization	An access determination that the Department of Energy (DOE) or Nuclear Regulatory Commission (NRC) grants based on a Tier 3 or successor background investigation as set forth in applicable national-level requirements and DOE directives. Within DOE and NRC, an ''L'' access authorization permits an individual who has an official ''need to know'' to access CONFIDENTIAL Restricted Data, SECRET and CONFIDENTIAL Formerly Restricted Data, SECRET and CONFIDENTIAL Transclassified Foreign Nuclear Information, or SECRET and CONFIDENTIAL National Security Information required in the performance of official duties. An ''L'' access authorization determination is required for individuals with a need to know outside of DOE, NRC, DOD, and in limited cases, National Aeronautics and Space Administration (NASA), to access Confidential Restricted Data.
Letter of Offer and Acceptance (LOA)	A contract signed by the U. S. Government and the purchasing government or international organization which provides for the sale of defense articles and defense services (to include training) from DOD stocks or through purchase under DOD-managed contracts with defense contractors.
Licensee	An individual or business organization that holds, or is issued, a license or franchise from a grantor to use the

L	
	grantor's name, administrative support, method of operation, or style in a specific area.
Limited Access Authorization (LAA)	Authorization for access to CONFIDENTIAL or SECRET information granted to non-U.S. citizens and immigrant aliens, which is limited to only that information necessary to the successful accomplishment of their assigned duties and based on a background investigation scoped for 10 years.
Limited Facility (Security) Clearance (FCL)	Grants the facility the right to obtain specific information related to a program, project, or contract. It may be granted to foreign-owned companies when there is an Industrial Security Agreement with the country of ownership, the release of classified information to the company is in conformity with U.S. National Disclosure Policy, and the GCA provides the DCSA with a letter of compelling need.
Limited Liability Company (LLC)	Both a business entity and an investment vehicle that seeks to provide some of the benefits of both the corporation and the partnership with ownership typically divided pro rata according to the members' investments. Regardless of the degree of ownership, a member of the LLC has the legal power to bind the LLC in the making of contracts and many other undertakings. The same authority to bind the entire enterprise applies to LLC managers. This legal authority exists whether or not the manager is also a member, and whether the manager has been authorized by the LLC to enter into the transaction. In most cases, the LLC is operated by a management board selected by the members; however, it may be operated by the members themselves. The management board may be made up of members, hired (non-member) management personnel, or a combination of both.
Loss	Classified information that is, or was, outside the custodian's control and the classified information cannot be located or its disposition cannot be determined.

Back to Top

M	
Mandatory Declassification Review (MDR)	The review of classified records for declassification in response to a declassification request that meets the requirements under DoDM 5230.30 section 3.5 of Reference (d).
Manufacturing License Agreement (MLA)	An agreement with prior written approval by the Directorate of Defense Trade Controls (e.g., a contract) whereby a U.S. person grants a foreign person an authorization to manufacture defense articles abroad and which involves: The export of technical data, or defense articles, or the performance of a defense service.

M	
	1. A foreign person using the technical data or defense articles previously exported by the U.S. person. 2. A foreign person using the technical data or defense articles previously exported by the U.S. person.
Marking Classified Information	The principal means to inform holders of classified information about specific protection requirements for that information. The marking and designation of classified information are the specific responsibilities of the original and derivative classifiers.
Material	Any product or substance on or in which information is embodied.
Matter	Anything in physical form that contains or reveals classified information.
Measures and Signatures Intelligence (MASINT)	An intelligence discipline built on capturing and measuring the intrinsic characteristics and components of an object or activity. These characteristics allow the object or activity to be detected, identified, or characterized every time it is encountered. If the 'target' vibrates, makes a sound, leaves a trace, or gets hot or cold, it could have an exploitable signature. MASINT measures the way things are and how they perform.
Media	Physical devices or writing surfaces including but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.
Memorandum of Agreement (MOA)	A written agreement between two or more parties or agencies outlining the terms and conditions of a collaborative effort or joint project. The purpose of an MOA is to establish a framework for cooperation and delineate the responsibility of each party.
Memorandum of Understanding (MOU)	A formal document describing the broad outlines of an agreement that two or more parties have reached through negotiations.
Mitigating Information	Personnel security information that tends to explain or refute factors that could otherwise support denial, revocation, or the granting of access to classified information with an exception.
Mitigation Instrument	A method applied to negate or mitigate risk of foreign ownership or control. Also referred to as a FOCI action plan. Includes Board Resolution, Security Control Agreement, Special Security Agreement, Proxy Agreement, and Voting Trust Agreement.
Mitigation/Negation Agreement	An agreement with information that tends to explain or refute factors that could otherwise support denial,

M	
	revocation, or the granting of access to classified information with an exception.
Multinational Industrial Security Working Group (MISWG)	An ad hoc international body currently comprised of the 28 NATO countries (less Iceland), plus Austria, Australia, Finland, Israel, New Zealand, Sweden, and Switzerland. It was created to harmonize security procedures for the protection of classified and controlled unclassified information involved in international cooperative programs. Procedures adopted by the MISWG countries are published in MISWG documents.
Multiple Facility Organization (MFO)	A legal entity (single proprietorship, partnership, association, trust, or corporation) composed of two or more contractors.
Multiple Sources	When using more than one classified source document in creating a derivative document.

Back to Top

N	
National Industrial Security Program (NISP)	Established by Executive Order 12829 for the protection of classified information released or disclosed to industry in connection with classified contracts. The NISP applies standards for the protection of classified information released or disclosed to contractors of all federal executive branch departments and agencies. Requirements of the NISP are stated in 32 CFR Part 117, also referred to as the National Industrial Security Program Operating Manual (NISPOM).
National Industrial Security Program Authorization Office (NAO)	Office within the Defense Counterintelligence and Security Agency (DCSA) that facilitates the Assessment and Authorization (A&A) process for classified information systems at cleared contractor facilities.
National Industrial Security Program (NISP) Contracts Classification System (NCCS)	The enterprise Federal information system application supporting DOD, the other Federal Agencies, and cleared industry in the NISP by facilitating the processing and distribution of contract security classification specifications for contracts requiring access to classified information.
National Industrial Security Program Operating Manual (NISPOM) – 32 CFR Part 117	Implements policy, assigns responsibilities, establishes requirements, and provides procedures consistent with Executive Order 12829, "National Industrial Security Program;" Executive Order 10865, "Safeguarding Classified Information within Industry;" and 32 Code of Regulation Part 2004, "National Industrial Security Program." That guidance outlines the protection of classified information that is disclosed to, or developed by contractors, licensees, grantees, or certificate holders to prevent unauthorized disclosure.
National Industrial Security System (NISS)	The Defense Counterintelligence and Security Agency (DCSA) System of Record for industrial security

N	
	oversight accessible by industry, Government, and DCSA personnel.
National Intelligence	All intelligence, regardless of the source, including information gathered within or outside the United States (U.S.) that: 1. Pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and. 2. That Involves: (i) threats to the U.S., its people, property, or interests. (ii) the development, proliferation, or use of weapons of mass destruction; or (iii) any other matter bearing on United States national or homeland security."
National Interest Determination (NID)	A written statement by the GCA affirming that the release of proscribed information to a company operating under an SSA will not harm the national security interests of the United States.
National of the United States	A person who owes permanent allegiance to the United States (U.S.). All U.S. citizens are U.S. nationals; however, not all U.S. nationals are U.S. citizens (for example, persons born in American Samoa or Swains Island).
National Security	Those activities which are directly concerned with the foreign relations of the United States, or protection of the Nation from internal subversion, foreign aggression, or terrorism.
National Security Adjudicative Guidelines	Guidelines established for determining eligibility for access to classified information. These guidelines are in accordance with the ODNI Security Executive Agent Directive (SEAD) 4, National Security Adjudicative Guidelines.
National Security Background Investigation	Any investigation required for the purpose of determining the eligibility of DOD military and civilian personnel, contractor employees, consultants, and other persons affiliated with the DOD for access to classified information, acceptance or retention in the Military Departments, assignment or retention in sensitive duties, or other designated duties requiring such investigation. It also includes investigations of allegations that arise subsequent to adjudicative action and require resolution to determine an individual's current eligibility for a national security position.
National Security Eligibility	Eligibility for access to classified information or to hold a sensitive position. This includes access to sensitive compartmented information, restricted data, and controlled or special access program information.

N	
National Security Information	Information that follows E.O. 13526 requires protection against unauthorized disclosure and is so marked when in documentary form.
National Security Threat	An entity capable of aggression or harm to the United States.
National Technology and Industrial Base (NTIB)	The industrial bases of the United States, Australia, Canada, and the United Kingdom.
National Technology and Industrial Base (NTIB) Entity	A subsidiary located in the United States for which the ultimate parent entity and any intermediate parent entities are in a country that is part of the national technology and industrial base (as defined in section 2500 of title 10, United States Code). It is subject to the foreign ownership, control, or influence requirements of the National Industrial Security Program.
Nationally Recognized Testing Laboratory (NRTL)	When the Occupational Safety and Health Administration recognize a private sector organization's ability to certify certain products. Each NRTL is recognized for a specific scope of test standards.
Naturalization	A process by which U.S. citizenship is granted to a foreign citizen or national after he or she fulfills the requirements established by Congress in the Immigration and Nationality Act (INA).
Naval Nuclear Propulsion Information (NNPI)	Classified or unclassified information concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear-powered ships and prototypes, including the associated shipboard and shore-based nuclear support facilities.
Need-to-Know (NTK)	A determination made by an authorized holder of classified information that a prospective recipient has a requirement for access to, knowledge, or possession of the classified information necessary to perform tasks or services essential to the fulfillment of a classified contract or program.
Network	A system of two or more Information Systems (IS) that can exchange data or information.
NOFORN	An intelligence control marking used to identify intelligence which an originator has determined falls under the criteria of Intelligence Community Directive (ICD) 710 and may not be provided in any form to foreign governments, international organizations, coalition partners, foreign nations, or immigrant aliens without foreign disclosure approval.
Non-critical Sensitive	Any civilian national security position that has the potential to cause significant or serious damage to the national security. This may include civilian national security positions.

N	
Non-DOD Executive Branch Agencies	The non-DOD agencies that have entered into agreements with DOD to receive National Industrial Security Program (NISP) industrial security services from DOD. A list of these agencies is on the Defense Counterintelligence and Security Agency website at https:// www.dcsa.mil.
Non-Federal Information System (defined in 32 CFR part 2002)	Any information system that does not meet the criteria for a federal information system.
Non-Working Hours (Non-WH)	Includes any time of day when cleared employees are not in the work area. A work force not working on a regularly scheduled shift.
North Atlantic Treaty Organization (NATO)	An intergovernmental military alliance that consists of 29 independent member countries across North America and Europe. NATO constitutes a system of collective defense whereby its member states agree to mutual defense in response to an attack by any external party. Three NATO members (the United States, France and the United Kingdom) are permanent members of the United Nations Security Council with the power to veto and are officially nuclear-weapon states.
North Atlantic Treaty Organization (NATO) Information	Information bearing NATO markings, indicating the information is the property of NATO, access to which is limited to representatives of NATO and its member nations unless NATO authority has been obtained to release it outside of NATO.
Nuclear Weapon Data	Restricted Data or Formerly Restricted Data concerning the design, manufacture, or utilization (including theory, development, storage, characteristics, performance, and effects) of nuclear explosives, nuclear weapons, or nuclear weapon components, including information incorporated in or related to nuclear explosive devices. Nuclear weapon data is matter in any combination of documents or material, regardless of physical form or characteristics.

Back to Top

O	
Office of the Chief Information Officer (OCIO)	A job title commonly given to the most senior executive in an enterprise who works with information technology and computer systems in order to support enterprise goals.
Office of the Director of National Intelligence (ODNI)	The U.S. Government agency that retains authority over access to intelligence sources and methods. The ODNI is also the U.S. Government national authority responsible for developing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of national security investigations and adjudications relating to determinations of eligibility for access to classified information or eligibility to hold a sensitive position, as well as other security duties as delineated in E.O. 13467.

O	
One-time Visit Authorization	Permits contact between a foreign national and a Department of Defense (DOD) Component or DOD contractor facility for a single, short-term occasion (normally less than 30 days) for a specified purpose.
Open Source	Any person or group that provides information without the expectation of privacy—the information, the relationship, or both is not protected against public disclosure.
Open Source Intelligence (OSINT)	Gathers information that is legally and publicly available, including information from the news media and internet.
Open Storage Area	An area constructed in accordance with §32 CFR 2001.53 and authorized by the agency head for open storage of classified information.
Operations Security (OPSEC)	A process of identifying critical information and analyzing friendly actions attendant to military operations and other activities to: 1. Identify actions that can be observed by adversary intelligence systems. 2. 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. 3. Determine which of these represent an unacceptable risk. 4. Select and execute countermeasures that eliminate the risk to friendly actions and operations or reduce it to an acceptable level.
Original Classification	An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure. Only United States Government (USG) officials who have received designation in writing may apply an original classification to information.
Original Classification Authority (OCA)	An individual authorized in writing by the President, the Vice President, agency heads, or other officials designated by the President to classify information in the first instance.

Back to Top

P	
Paraphrasing/Restating	Taking information from an authorized source of classification guidance and re-wording it in a new or different document.
Parent	An entity that owns a majority of another entity's voting securities.
Performance Work Statement (PWS)	States the work in terms of outcomes or results rather than methods of performance. It defines measurable performance standards and financial incentives.

P	
Perimeter Controls	Entry and exit inspections that deter and detect the introduction or removal of classified information from a facility without proper authority.
Periodic Reinvestigation (PR)	A former process of national security investigation conducted to update a previously completed investigation on persons holding a national security position or performing national security duties to determine whether that individual continues to meet national security requirements. Replaced by Continuous Vetting.
Personally Identifiable Information (PII)	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.
Personnel Security (PERSEC)	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) Clearance (PCL)	An administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted.
Personnel Security Clearance Certificate (PSCC)	Employees of cleared U.S. defense contractors must have the appropriate level PSCC to participate in a NATO program or contract, or to visit a NATO entity.
Personnel Security Investigation (PSI)	An inquiry into the activities of an individual. It is designed to discover pertinent information pertaining to a person's suitability for a position of trust as related to loyalty, character, emotional stability, and reliability.
Personally Identifiable Information (PII)	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information, that is linked or linkable to a specific individual.
Physical Security	The security discipline concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.
Portion Markings	Identify the classification levels of individual sections of a document.
Preliminary Inquiry	Immediately upon receipt of a security violation report involving classified information, the contractor will initiate a preliminary inquiry to ascertain all of the circumstances surrounding the presumed loss, compromise, or suspected compromise, including validation of the classification of the information.
Prime Contract	A contract awarded by a Government Contracting Authority (GCA) to a contractor for a legitimate United States Government (USG) purpose.

P	
Prime Contractor	The contractor who receives a prime contract from a Government Contracting Authority (GCA).
Privacy Act	Establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of PII about individuals that is maintained in systems of records by federal agencies.
Privately-held Corporations	Also called "close" or "closely-held" companies and are owned by a small number of individuals, often family members. Shares in the company are not available to the general public. Those who own the shares of voting stock in the corporation have ultimate control over the company.
Privileged User	A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
Procurement	The process of finding and agreeing to terms, and acquiring goods, services, or works from an external source, often via a tendering or competitive bidding process.
Program Protection Plan (PPP)	A risk-based, comprehensive, living plan to protect Critical Program Information (CPI) that is associated with a Research, Development and Acquisition (RDA) program.
Program Security Instruction (PSI)	A security document, negotiated between the security officials of governments participating in a cooperative program, which is used to standardize and provide advance government approval for the specific security arrangements to be used in support of the program, i.e., a program security standard operating procedure (SOP). The PSI is comprised of agreed procedures to be used in the program (e.g., visit procedures, hand carry procedures, transportation plans). It also may be used to levy Program Protection Plan countermeasures requirements on foreign participants in a cooperative program. A PSI may be used for commercial programs, subject to the approval of the Defense Counterintelligence and Security Agency.
Program Manager (PM)	Individual with assigned responsibility for maintaining the appropriate operational security posture for a classified contract.
Proscribed Information	1. TOP SECRET information; 2. COMSEC information or material, excluding controlled cryptographic items when un-keyed or utilized with unclassified keys; 3. Restricted Data (RD); 4. SAP information; or 5. SCI.
Protective Security Service (PSS)	A transportation protective service provided by a cleared commercial carrier qualified by DOD's Surface

P	
	Deployment and Distribution Command to transport SECRET shipments.
Proxy Agreement (PA)	A mitigation agreement in which the foreign owner maintains ownership of the company but relinquishes most of his or her rights of ownership. All voting rights are transferred to Proxy Holders, individuals who have no prior involvement with the foreign owner or the company.
Public Domain	The state of being generally accessible or available to the public per Reference (s) or section 552 of Title 5, United Sates Code (U.S.C.) (Reference (an)).
Publicly-held Corporations	Make their ownership shares available to the general public. The entities that hold these shares own the company. The stockholders that own the voting stock control the corporation.

Back to Top

Q	
Q Access Authorization	An access determination granted by the Department of Energy (DOE) or Nuclear Regulatory Commission (NRC) based on a Tier 5 or successor background investigation as set forth in applicable national-level requirements and DOE directives. Within DOE and the NRC, a ‘‘Q’’ access authorization permits an individual with an official ‘‘need to know’’ to access TOP SECRET, SECRET, and CONFIDNETIAL Restricted Data, Formerly Restricted Data, Trans-classified Foreign Nuclear Information, National Security Information, or special nuclear material in Category I or II quantities as required in the performance of official duties. A ‘‘Q’’ access authorization is required for individuals with a need to know outside of DOE, NRC, DOD, and in a limited case, National Aeronautics and Space Administration (NASA), to access TOP SECRET and SECRET Restricted Data.
Questionnaire for National Security Positions (SF-86)	The standard form that the DOD uses for most national security background investigations. The form is generally completed electronically via a secure system.
Questionnaire for Non-Sensitive Positions (SF-85)	Developed by the Office of Personnel Management for background investigations and reinvestigations. Completed by the applicant, the Questionnaire for Non-Sensitive Positions.
Questionnaire for Public Trust Positions (SF-85P)	Developed by the Office of Personnel Management for background investigations and reinvestigations. Completed by the applicant, the Questionnaire for Public Trust Positions.

Back to Top

R	
Receipt	A written or digitally signed acknowledgment of having received a specified item, information, freight, or documents.
Reciprocity	The acknowledgement and acceptance of an existing background investigation conducted by an authorized investigative agency, the acceptance of a national security eligibility adjudication determined by an authorized adjudicative agency, and the acceptance of an active national security eligibility determination granted by an executive branch agency.
Recurring Visit Authorization	Permits intermittent visits by a foreign national to a Department of Defense (DOD) Component or DOD contractor facility over a specified period of time for a Government-approved license, contract, or agreement, or other program when the information to be disclosed has been defined and approved for disclosure in advance by the U.S. Government.
Regrade	To raise or lower the classification assigned to an item of information.
Reinvestigation	A national security investigation conducted to update a previously completed investigation on persons holding a national security position or performing national security duties to determine whether that individual continues to meet national security requirements. New reinvestigation requests, as directed per the CE program/CV model, are screened using a risk management-based approach, where an individual's Questionnaire for National Security Positions (SF-86) is analyzed using deferment protocols and is identified for either enrollment in CE or submission to an Investigative Service Provider (ISP) for a reinvestigation.
Remote Terminal	A device communicating with an automated information system from a location that is not within the central computer facility.
Request for Proposal (RFP)	A formal negotiated solicitation that results in a formal contract award.
Request for Quote (RFQ)	A solicitation used in negotiated acquisition to communicate Government requirements to prospective contractors and to solicit a quotation. A response to an RFQ is not an offer; however, it is informational in character.
Request for Visit (RFV)	Required for incoming international visits. The RFV may be submitted through the sponsoring government's embassy in Washington, D.C. or by the sponsoring organization using the automated Foreign Visits System (FVS) and IVP procedures. The cognizant U.S. Government agency approves or rejects the RFV.
Restricted Area	A controlled access area established to safeguard classified material that, because of its size or nature, cannot be adequately protected during working hours by

R	
	the usual safeguards, but is capable of being stored during non-working hours in an approved repository or secured by other methods approved by the CSA.
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 does not include data declassified or removed from the RD category pursuant to section 142 of the Atomic Energy Act (AEA) of 1954.
Revealed By	The concept applied when derivative classifiers incorporate classified information from an authorized source of classification guidance into a new document which is not clearly or explicitly stated in the source document.
Risk	The probability of loss from an attack or adverse incident; it is a function of threat (adversaries' capabilities, intentions, and opportunities) and vulnerability (the inherent susceptibility to attack). Risk may be quantified and expressed in terms such as loss of life, dollars, resources, programmatic impact, etc.
Risk Analysis	A method by which individual vulnerabilities are compared to perceived or actual security threat scenarios in order to determine the likelihood of compromise of critical information.
Risk Assessment	A systematic examination of risk using disciplined processes, methods, and tools. A risk assessment provides an environment for decision makers to evaluate and prioritize risks continuously and to recommend strategies to remediate or mitigate those risks.

Back to Top

S	
Sabotage	An act or acts with the intent to injure, interfere, or obstruct the national defense of a country by willfully injuring, destroying, or attempting to destroy any national defense or war materiel, premises, or utilities, to include human or natural resources.
Safeguarding	Approval to allow the storage of classified information within a contractor's facility at the same classification level as the company's FCL, or lower. Contractors will be responsible for safeguarding classified information in their custody or under their control, with approval for such storage of classified information by the applicable CSA. Individuals are responsible for safeguarding classified information entrusted to them. Contractors will provide the extent of protection to classified information sufficient to reasonably protect it from loss or compromise.
Scheduled Declassification	A set date or event, determined by the Original Classification Authority (OCA), which will occur within 25 years of the original classification date.

S	
Scope	The time period to be covered and the sources of information to be contacted during the prescribed course of a national security investigation.
SECRET	The classification level applied to information; the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security that the OCA is able to identify or describe.
SECRET Internet Protocol Router Network (SIPRNet)	The worldwide SECRET level packet switch network that uses high-speed internet protocol routers and high-capacity Defense Information Systems Network circuitry.
Secure (Electronic) System	A secure, web-based automated system that collects and facilitates the timely and accurate processing of background investigation requests, fingerprints, and demographic information. An electronic tool for self-reporting biographic details, declarations, clarifications, and mitigating information necessary to conduct background investigations for suitability and national security eligibility determinations.
Secure Web Fingerprint Transmission (SWFT):	Is a web-based system that enables cleared defense industry users to submit e-fingerprints for applicants who require investigation for a personnel security clearance.
Security Assurance	The written confirmation requested by, and exchanged between, governments regarding the security clearance level or eligibility for clearance of their employees, contractors, and citizens. It includes a statement by a responsible official of a foreign government that the original recipient of U.S. classified information possesses the requisite security clearance, is approved by his or her government for access to information of the security classification involved on behalf of the foreign government, and that the recipient will comply with any security requirements specified by the U.S. In the case of contractors, security assurance includes a statement concerning the level of storage capability.
Security Classification Guidance (SCG)	Any instruction or source that sets out the classification of a system, plan, program, mission, or project. Initially issued by an Original Classification Authority to document and disseminate classification decisions under their jurisdiction.
Security Classification Guide (SCG)	A document issued by an authorized original classifier that identifies the elements of information regarding a specific subject that must be classified, prescribes the level and duration of the classification, and appropriate declassification instructions. Classification guides for contractors are referenced in the Contract Security Classification Specification (DD Form 254) and provided by the GCA.
Security Control Agreement (SCA)	The mitigation generally used when a company is not effectively owned or controlled by a foreign interest (minority ownership) and the foreign interest is entitled to

S	
	representation on the company's governing board. The foreign owner still maintains his or her voice in the management of the business through an Inside Director but is denied access to classified or controlled information.
Security-in-depth	A determination made by the CSA that a contractor's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include, but are not limited to, use of perimeter fences, employee and visitor access controls, use of an Intrusion Detection System (IDS), random guard patrols throughout the facility during nonworking hours, closed circuit video monitoring, or other safeguards that mitigate the vulnerability of open storage areas without alarms and security storage cabinets during nonworking hours.
Security Incident	A security compromise, infraction, or violation.
Security Infraction	A security incident that is not in the best interest of security and does not involve the loss, compromise, or suspected compromise of classified information.
Security Manager	Manages and implements the DOD activity's information security program on behalf of the activity head, to whom he or she shall have direct access.
Security Rating	The National Industrial Security Program (NISP) contractor's security posture is rated as a result of each security review. This rating is a summary description for purposes of the contractor's compliance with the requirements National Industrial Security Program Operating Manual (NISPOM), Industrial Security Letters (ISLs), any other applicable guidance, and the contractor's effectiveness in protecting classified information from unauthorized disclosure or compromise.
Security Review	A review of a contractor's security program done by a DCSA IS Rep. The security review can be done individually or as a team. It evaluates and rates NISPOM compliance, assesses actions taken to ensure the contractor adequately mitigates vulnerabilities, advises the contractor on how to achieve and maintain an effective security program, and considers the following: what the facility is protecting related to a classified contractor program and how the contractor protects the associated elements, approach vectors applicable to the facility and measures in place to counter the potential threat, and internal processes throughout the classified contract deliverable lifecycle.
Security Incident Report	Formal investigation of a possible loss, compromise, or suspected compromise of classified information.
Security Training Education and Professionalization Portal (STEPP)	The learning management system used by the Center for Development of Security Excellence (CDSE). STEPP is where the list of courses, student information, and course transcripts are maintained.

S	
Security Violation	A failure to comply with the policy and procedures established by the NISPOM that reasonably could result in the loss or compromise of classified information.
Security Vulnerability	All instances of non-compliance with the National Industrial Security Program Operating Manual (NISPOM) that are not acute or critical vulnerabilities. Any weakness that can be exploited by an adversary to gain access to an asset. Vulnerabilities can result from, but are not limited to, the following: building characteristics; equipment properties; personal behavior; locations of people, equipment, and buildings; or operational and personnel practices.
Self-Inspection	The NISPOM requires all participants in the National Industrial Security Program (NISP) to conduct their own self-inspections to include an insider threat self-assessment. The self-inspection requires a review of the Industrial Security Program and security procedures established within a company and validates that they not only meet NISPOM requirements, but are effectively implemented by cleared employees. Self-inspections should be tailored to the classified needs of the cleared company and are conducted to ensure the continued protection of national security.
Senior Management Official (SMO)	An entity employee with ultimate authority over the facility's operations and the authority to direct actions necessary for the safeguarding of classified information in the facility. This includes the authority to direct actions necessary to safeguard classified information when the access to classified information by the facility's employees is solely at other contractor facilities or USG locations.
Sensitive Compartmented Information (SCI)	A subset of Classified National Intelligence concerning or derived from intelligence sources, methods, or analytical processes that must be protected within formal access control systems established by the Director of National Intelligence.
Sensitive Compartmented Information Facility (SCIF)	An accredited area, room, group of rooms, or installation where sensitive compartmented information may be stored, used, discussed, and/or electronically processed. Where procedural and physical measures prevent free access for persons unless they have been formally indoctrinated for the particular sensitive compartmented information authorized for use or storage within the SCIF.
Sensitive Information	Information that the loss, misuse, unauthorized access, or modification of could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under U.S. Code.
Sensitive Position	Any position within, or in support of, an agency in which the occupant could bring about, by virtue of the nature of the position, a material adverse effect on

S	
	national security regardless of whether the occupant has access to classified information and regardless of whether the occupant is an employee, military service member, or contractor.
Shipper	One who releases custody of material to a carrier for transportation to a consignee. (See also ‘‘Consignor.’’)
Signals Intelligence (SIGINT)	Involves the collection of electronic signals, including phone calls and emails.
Social Engineering	An attempt to trick someone into revealing information that could be used to attack systems or networks.
Sole Proprietorship	The simplest type of business structure; a business owned by one individual who is liable for the debts and other liabilities incurred in the operation of the business.
Solicitation	Any request to submit offers or quotations to the Government. Solicitations under sealed bid procedures are called Invitations For Bids (IFB). Solicitations under negotiated procedures are called Requests For Proposals (RFP). Solicitations under simplified acquisition procedures may require submission of either a quotation or an offer.
Source Document	An existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.
Special Access Program (SAP)	Any program that is established to control access, distribution, and to provide protection for particularly sensitive classified information beyond that normally required for TOP SECRET, SECRET, or CONFIDENTIAL information. An SAP can be created or continued only as authorized by a senior agency official delegated such authority pursuant to E.O. 13526.
Special Category System	A tactical, embedded, data acquisition, legacy, or special purpose Information System (IS) requiring an alternative set of controls not readily available in typical systems since some IS are incapable of alteration by users and are designed and implemented to provide a very limited set of predetermined functions. These systems are characterized by some common features. First, and most importantly, there are no general users on the system. Second, there is no user code running on the system. In addition, if an IS meets the criteria of a legacy system, upgrading the systems in order to meet the baseline security controls may outweigh the benefit of the additional control and continued technological enhancements. Examples include some data acquisition systems and some other special purpose test type systems, such as those embedded as an integral element of a larger system that are used to perform or control a specific function (such as control systems or weapons systems) concurrently with the design and development of the system.

S	
Special Security Agreement (SSA)	A security agreement that may be imposed in cases of majority foreign ownership or control. The foreign owner has a voice in the management of the business through an Inside Director. The SSA is the most common mitigation agreement.
Special-sensitive	A special-sensitive civilian national security position is one with potential for inestimable damage to the national security or for inestimable adverse impact to the efficiency of the Department of Defense or the Military Departments.
Spillage	Occurs when classified data is introduced on an information system not approved for that level of information.
Standard Form (SF) 86	The standard form that the DOD uses for most national security background investigations. The automated version of the SF 86 is the e-QIP.
Standard Form (SF)-700	Security Container Information used to maintain a record for each container and to record the combination.
Standard Form SF)-701	Activity Security Checklist used to record checks of work areas at the end of each working day.
Standard Form (SF)-702	Security Container Check Sheet used to record the securing of vaults, rooms, and containers used for storing classified material.
Standard Form (SF)-703	Cover sheet for TOP SECRET material.
Standard Form (SF)-704	Cover sheet for SECRET material.
Standard Form (SF)-705	Cover sheet for CONFIDENTIAL material.
Standard Practice Procedures (SPP)	A document prepared by a contractor that establishes the rules for the contractor's operations and involvement with classified information at the contractor's facility.
Statement of Work (SOW)	Designed to describe not only what is to be done, but also how it is to be done.
Storage Container	See Approved Security Container.
Subcontract	Any contract entered into by a contractor to furnish supplies or services for performance of a prime contract or a subcontract. It includes a contract, subcontract, purchase order, lease agreement, service agreement, request for quotation (RFQ), request for proposal (RFP), invitation for bid (IFB), or other agreement or procurement action between contractors that requires or will require access to classified information to fulfill the performance requirements of a prime contract.
Subcontractor	A supplier, distributor, vendor, or firm that enters into a contract with a prime contractor to furnish supplies or services to or for the prime contractor or another subcontractor. For the purposes of the NISPOM, each subcontractor will be considered as a prime contractor in relation to its subcontractors.
Subsidiary	An entity in which another entity owns a majority of its voting securities.

S	
Subversion	An attempt to transform the established social order and its structures of power, authority, and hierarchy.
Supply Chain	The linked activities associated with providing materiel from a raw material stage to an end user as a finished product.
Supply Chain Risk Management (SCRM)	The management of supply chain risk whether presented by the supplier, the supplied product and its sub-components, or the supply chain (e.g., packaging, handling, storage, and transport).
Suspected Compromise	Occurs whenever identifiable classified information has been made available to unauthorized individual(s) who may have gained access to the information.
Suspicious Contact	Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee. All contacts by cleared employees with known or suspected intelligence officers from any country, or any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence services of another country.
Suspicious Contact Reports (SCRs)	A report of Counterintelligence (CI) concern that likely represents efforts by an individual to obtain illegal or unauthorized access to classified information or technology.
System for Award Management (SAM)	Secure web portal that consolidates various Government acquisition and award capabilities into one system.
System Security Plan(SSP)	Describes the planned security tasks required to meet system or network security requirements.
System Software	Computer programs that control, monitor, or facilitate use of the information system; for example, operating systems, programming languages, communication, input-output controls, sorts, security packages, and other utility-type programs. Also includes off-the-shelf application packages obtained from manufacturers and commercial vendors such as word processing, spreadsheets, data base management, graphics, and computer-aided design.
Systematic Declassification	Review of classified information that has been exempted from automatic declassification.

Back to Top

T	
Technical Data	1. Information, other than software, which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions, or documentation. 2. Classified information relating to defense articles and defense services on the U.S. Munitions List

T	
	and 600-series items controlled by the Commerce Control List. 3. Information covered by an invention secrecy order. 4. Software directly related to defense articles.
Technology	The information and know-how (whether in tangible form, such as models, prototypes, drawings, sketches, diagrams, blueprints, or manuals, or in intangible form, such as training or technical services) that can be used to design, produce, manufacture, utilize, or reconstruct goods. This includes computer software and technical data, but not the goods themselves, or the technical information and know-how that can be used to design, produce, manufacture, use, or reconstruct goods, including technical data and computer software.
Technology Control Plan (TCP)	A detailed plan to control access by foreign national employees and by foreign national visitors on an extended visit authorization at a DOD cleared contractor facility.
TEMPEST	The protection of sensitive information being compromised from electronic equipment producing emissions, including unintentional radio or electrical signals, sounds, and vibrations.
Terrorism	The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.
Threat	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or Denial of Service (DOS).
TOP SECRET	The classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the OCA is able to identify or describe.
Trade Secret	All forms and types of financial, business, scientific, technical, economic, or engineering information including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if: (a) the owner thereof has taken reasonable measures to keep such information secret; and (b) the information derives independent economic value, actual or potential, from not being generally known to and not being readily ascertainable through proper means by the public.

T	
Trans-classified Foreign Nuclear Information (TFNI)	Classified information concerning the nuclear energy programs of other nations (including subnational entities) removed from the Restricted Data (RD) category under section 142(e) of the Atomic Energy Act after the Department of Energy (DOE) and the Director of National Intelligence jointly determine that it is necessary to carry out intelligence-related activities under the provisions of the National Security Act of 1947, as amended, and that it can be adequately safeguarded as National Security Information instead. This includes information removed from the RD category by past joint determinations between DOE and the CIA. TFNI does not include information transferred to the United States under an Agreement for Cooperation under the Atomic Energy Act or any other agreement or treaty in which the United States agrees to protect classified information.
Transmission	The sending of information from one place to another by audio, microwave, laser, or other non-connective methods, as well as by cable, wire, or other connective medium. Transmission also includes movement involving the actual transfer of custody and responsibility for a document or other classified material from one authorized addressee to another.
Transshipping Activity	A Government activity to which a carrier transfers custody of a freight for reshipment by another carrier to the consignee.

Back to Top

U	
Unauthorized Access	A person not authorized to have access to specific classified information in accordance with the requirements of the NISPOM.
Unauthorized Disclosure	A communication, confirmation, acknowledgement, or physical transfer of classified information, including the facilitation of, or actual giving, passing, selling, publishing, or in any way making such information available to an unauthorized recipient.
Unauthorized Person	A person not authorized to have access to specific classified information in accordance with the requirements in 32 CFR Part 117.
Under Secretary of Defense for Acquisition and Sustainment (USD (A&S))	This office within the Department of Defense establishes acquisition policy, procedures, and guidance in coordination with Under Secretary of Defense for Intelligence and Security (USD (I&S)).
Under Secretary of Defense for Intelligence and Security (USD (I&S))	Office within the Department of Defense that is responsible for overseeing NISP policy and management.
Underwriters Laboratory (UL)	Is a global, independent, not-for-profit product safety certification organization that publishes a vast number of standards.

U	
Underwriters Laboratory (UL) 2050 Standards	These standards are established by the Underwriters Laboratory, Inc. (UL) in cooperation with the U.S. Government.
United States (U.S.)	The 50 states and the District of Columbia.
United States (U.S.) and its territorial areas	The 50 states, the District of Columbia, Puerto Rico, Guam, American Samoa, the Virgin Islands, Wake Island, Johnston Atoll, Kingman Reef, Palmyra Atoll, Baker Island, Howland Island, Jarvis Island, Midway Islands, Navassa Island, and Northern Mariana Islands.
United States (U.S.) Classified Cryptographic Information	A cryptographic key and authenticators that are classified and designated as TOP SECRET CRYPTO or SECRET CRYPTO. This means all cryptographic media that embody, describe, or implement classified cryptographic logic, to include, but not limited to, full maintenance manuals, cryptographic descriptions, drawings of cryptographic logic, specifications describing a cryptographic logic, and cryptographic software, firmware, or repositories of such software such as magnetic media or optical disks.
United States (U.S.) Person	A United States citizen, an alien known by the intelligence agency considered to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments
Upgrade	A determination that certain classified information, in the interest of national security, requires a higher degree of protection against unauthorized disclosure than currently provided, coupled with a change to the classification designation to reflect the higher degree.

Back to Top

V	
Vetting	A process to review the background of an individual to determine (or has been determined) whether that individual meets (or continues to meet) applicable requirements to be eligible for access to classified information or to hold a sensitive position.
Visit Authorization Letter (VAL)	When a visit requires access to classified information, the host contractor must verify the visitor's PCL level. Verification of a visitor's PCL may be accomplished by a review of the DOD personnel security system of record that contains the information or by a Visit Authorization Letter (VAL) provided by the visitor's employer. A VAL can also be referred to as a Visit Authorization Request (VAR).
Visit Authorization Request (VAR)	See definition of Visit Authorization Letter.
Voting Securities	Any securities that presently entitle the owner or holder thereof to vote for the election of directors of the issuer or, with respect to unincorporated entities, individuals exercising similar functions.

V	
Voting Trust Agreement (VTA)	The most restrictive mitigation agreement. Under a VTA, the foreign owner transfers ownership of the company to the Voting Trustees.

Back to Top

W	
Waivers	Temporary exclusions or deviations put in place when classified information cannot be safeguarded to the standards or requirements specified in Department of Defense Manual (DODM) DODM 5200.01.
Working Hours	The period of time when: 1. There are employees present in the specific area where classified material is located, a work force on a regularly scheduled shift, as contrasted with employees working within an area on an overtime basis outside of the scheduled work shift. 2. The number of employees in the scheduled work force is sufficient in number and so positioned to be able to detect and challenge the presence of unauthorized personnel. This would, therefore, exclude janitors, maintenance personnel, and other individuals whose duties require movement throughout the facility.
Working Papers	Documents or materials, regardless of the media, which are expected to be revised prior to the preparation of a finished product for dissemination or retention.
Workplace Violence	Any act of violent behavior, threats of physical violence, harassment, intimidation, bullying, verbal or non-verbal threat, or other threatening, disruptive behavior that occurs at or outside the work site.

Back to Top

X

Back to Top

Y

Back to Top

Z

Back to Top