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.
Adjudication	The adjudication process is based on decisions made by applying a standard set of guidelines to an individual's specific circumstances.
Adverse Information	Any information that adversely reflects on the integrity or character of a cleared employee, that suggest that his or her ability to safeguard classified information may be impaired, that his or her access to classified information clearly may not be in the interest of national security, or that the individual constitutes as insider threat.

Back to Top

B

Back to Top

C	
Center for Development of Security Excellence (CDSE)	A nationally accredited, award-winning directorate within the Defense Counterintelligence and Security Agency (DCSA). CDSE provides security, training and certification products and services for the Department of Defense, (DOD) and industry.
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 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	Consists of three elements. What needs to be protected, how much protection is required and declassification of National Security Information (NSI). It is a joint responsibility between the contractor and the U. S. government.
Classification Level	Classification levels are applied to national security information 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.
C	
Classified Contract	Any contract requiring access to classified information by a contractor and its employees 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" also are 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 Information	Official information that has been determined, pursuant to E.O. 13526 or any predecessor order to require protection against unauthorized disclosure in the interest of national security which has been designated. The term includes National Security Information (NSI), Restricted Data (RD) and Formerly Restricted Data (FRD).
Classified Information Nondisclosure Agreement (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.
Clearance	Formal security determination by an authorized adjudicative office that an individual has authorized access, on a need to know basis, to a specific level of collateral classified information (TOP SECRET, SECRET, CONFIDENTIAL).
Cleared Contractor/Company	All contractors who safeguard classified information disclosed during all phases of the contracting, licensing, and grant process, including bidding, negotiation, award, performance, and termination. Any industrial, educational, commercial, or other entity that has been granted an Facility Clearance (FCL) by a Cognizant Security Agency (CSA) and participating in the National Industrial Security Program (NISP).
Cleared Employees	All 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 appropriated agency head who are granted Personnel Security Clearances (PCL) and are being processed for PCLs.
Cognizant Security Agency (CSA)	Agencies of the Executive Branch that have been authorized by E.O. 12829 to establish an industrial security program to safeguard classified information under the jurisdiction of those agencies when disclosed or released to U.S. industry. These agencies are the DOD, Department of Energy (DOE), Office of the Director of

	National Intelligence (ODNI), Nuclear Regulatory Commission (NRC), and Department of Homeland Security (DHS).
Cognizant Security Office (CSO)	The organizational entity delegated by the Head of a CSA to administer industrial security on behalf of the CSA.
C	
Company	A generic and comprehensive term which may include sole proprietorships, individuals, partnerships, corporations, societies, associations, and organizations usually established and operating to carry out a commercial, industrial or other legitimate business, enterprise, or undertaking.
Compromise	An unauthorized disclosure of classified information.
CONFIDENTIAL	The classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.
Contractor	Licensees, grantees, and certificate holders, to the extent legally and practically possible within the constraints of applicable law and the Code of Federal Regulations.
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.
Counterintelligence (CI)	Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.
Counterintelligence 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.
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 through the use of computer networks that result in an actual or potentially adverse effect on an information system or the information residing therein.

Back to Top

D	
Defense (Cleared) Contractor	A subset of contractors cleared under the NISP who have classified contracts with the DOD.

Defense Counterintelligence and Security Agency (DCSA)	The DCSA is an agency of the DOD with field offices throughout the U.S. and provides the military services, defense agencies, other federal agencies and cleared contractor facilities with security support services. DCSA is the security agency in the federal government dedicated to protecting America's trusted workforce and trusted workspaces — real or virtual. DCSA joins two essential missions: Personnel Vetting and Critical Technology Protection, supported by Counterintelligence and Training, Education and Certification functions. DCSA services over 100 federal entities, oversees 10,000 cleared companies, and conducts approximately 2 million background investigations each year.
D	
Department of Defense (DOD)	The DOD is an executive branch department of the federal government of the U.S. charged with coordinating and supervising all agencies and functions of the government concerned directly with national security and the U.S. Armed Forces. The major elements of these forces are the Army, Navy, Marine Corps, and Air Force.
Document	Any recorded information, regardless of the nature of the medium or the method or circumstances of recording.
DOD Personnel 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.
DOD 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.
Duties/position (for National Security)	Duties performed or position by individuals working for, or on behalf of, the Federal Government that are concerned with the protection of the United States (U.S) from foreign aggression or espionage, including 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	
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.

Employee	A person, other than the President and Vice President of the United States (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.
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), a specification location or facility, or the headquarters/official business location of the organization, depending upon the organization's business structure, the access needs involved, and the responsible CSA's procedures. The term "entity" as used in the NISPOM 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.
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.
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.

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.

F	
Facility (Security) Clearance (FCL)	An administrative determination that, from a security point of view, a company is eligible for access to classified information of a certain category (and all lower categories). FCL is also referred to as an entity eligibility determination.
FCL System of Record	An electronic system that is a repository of information about DOD cleared contractor facilities. The system has internal users (with full access) such as DCSA personnel and external users (with limited access). It offers a variety of functionality that facilitates the process for FCL requests, processing, and maintenance. Functions and features include but are not limited to the following: request an FCL, report a change condition, message your IS Rep, request a facility profile update, submit an FCL verification and submit an annual self-inspection certification.
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.
Foreign Government Information (FGI) (or material)	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 National	Any person who is not a citizen or nation of the U.S.
Federal Bureau of Investigation (FBI)	An intelligence-driven and threat-focused national security organization with both intelligence and law enforcement responsibilities—the principal investigative arm of the U.S. Department of Justice and a full member of the U.S. Intelligence Community.
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 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

F	
	which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts.

Back to Top

G

Back to Top

H

Back to Top

I	
Impact	A step in the original classification process that assesses the probable operational, technological, and resources of classification.
Individual Culpability	An individual responsible for a security violation plus evidence of deliberate disregard, gross negligence and a pattern of negligence or carelessness.
Industrial Security	That portion of information security concerned with the protection of classified information in the custody of U.S. industry.
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.
Information	Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics.
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 otherwise manipulating data, information, and textual material.
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).
Insider	Cleared contractor personnel with authorized access to any government 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 U.S. national security. Insider threats may include harm to contractor or program information, to the extent that the information impacts the contractor or agency's obligations to protect classified NSI.
Insider Threat Program Senior Official (ITPSO)	A U.S. citizen employee, appointed by a contractor who will establish and execute an insider threat program.

I	
Investigation	The action of investigating something or someone; formal or systematic examination or research

Back to Top

J

Back to Top

K	
Key Management Personnel (KMP)	A company's Senior Management Official (SMO), FSO, ITPSO, and all other company officials who either hold majority interest or stock, or have (direct or indirect) authority to influence or decide matters affecting the management or operations of the company or classified contract performance. Essential KMPs require an eligibility determination before a facility is granted an FCL. Other applicable KMPs may be formally excluded from classified access.

Back to Top

L	
Limited Access Authorization (LAA)	A security access authorization to CONFIDENTIAL or SECRET information granted to non-U.S. citizens requiring only limited access sin the course of their regular duties.
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	
Material	Any product or substance on or in which information is embodied.

Back to Top

N	
National Industrial Security Program (NISP)	The NISP was established by E.O. 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 the NISPOM.
National Industrial Security Program Operating Manual (NISPOM)	A manual issued in accordance with the NISP that prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information.
National Security	The national defense of foreign relations of the U.S. national security, including defense against transnational terrorism.

N	
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 Eligibility	The status that results from a formal determination by an adjudication facility that a person meets the personnel security requirements for access to classified information or to occupy a national security position or one requiring the performance of national security duties.
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).
Network	A system of two or more Information Systems (IS) that can exchange data or information.

Back to Top

O

Back to Top

P	
Personnel Security	A security discipline that assesses the loyalty, reliability, and trustworthiness of individuals for initial and continued eligibility for access to classified information.
Personnel (Security) Clearance (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 PCL being granted. PCL is also referred to as national security eligibility determination.
Preliminary Inquiry	Secure the classified information, quickly gather all the facts, and determine if the classified information was subject to loss, compromise, or suspected compromise.
Prime Contractor	The contractor who receives a prime contract from a Government Contracting Authority (GCA).

Back to Top

Q

Back to Top

R	
Receipt	A written or digitally signed acknowledgment of having received a specified item, information, freight, or documents.
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

R	
	and expressed in terms such as cost in loss of life, dollars, resources, programmatic impact, etc.

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.
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 reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.
Security Clearance	A national security eligibility determination by competent authority that an individual is eligible for access to NSI, under the standards of NISPOM. Also called a clearance. The individual must have both eligibility and access to have a security clearance. Eligibility is granted by the adjudication facilities, and the access is granted by the individual agencies.
Security Container (approved)	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.
Security Incident	A security compromise, infraction, or violation.
Security Review	A review of a contractor security program done by a DCSA Industrial Security Representative. The Security Review can be done individually or as a team.
Security Training Education and Professionalization Portal (STEPP)	The learning management system used by CDSE. STEPP maintains a list of courses, student information and course transcripts.
Security Violation	Occurs when there is a knowing, willful, or negligent action that could reasonably be expected to result in the loss, suspected compromise, or compromise of classified information.
Security Vulnerability	All instances of non-compliance with the 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,

S	
	equipment, and buildings; or operational and personnel practices.
Self-Inspection	The NISPOM requires all participants in the 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)	The SMO is the contractor's official responsible for company policy and strategy. The SMO is a U.S. citizen employee occupying a position with ultimate authority over the facility's operations and directs actions necessary for the facility's safeguarding of classified information (even if the access to classified information by the facility's employees is solely at other contractor facilities or government locations).
Sensitive (Information/Position)	An agency, installation, person, position, document, material, or activity requiring special protection from the disclosure, loss, misuse, alteration, or destruction of which could cause embarrassment, compromise, or threat to the security of the sponsoring power and/or adversely affect national security or governmental interests.
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.
Subcontractor	A supplier, distributor, vendor, or firm that furnishes supplies or services to or for a prime contractor or another subcontractor, who enters into a contract with a prime contractor. Per NISPOM, each subcontractor will be considered as a prime contractor in relation to its subcontractors.
Subversion (or subversive activities)	An attempt to transform the established social order and its structures of power, authority, and hierarchy.
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

S	
	of an attempted exploitation by the intelligence services of another country.

Back to Top

T	
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.
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 (to National Security)	An entity capable of aggression or harm to the U.S.
TOP SECRET	The classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
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.

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 or physical transfer of classified national intelligence, including SCI, to an unauthorized recipient.
Unauthorized Person/Personnel	A person not authorized to have access to specific classified information in accordance with the requirements in NISPOM.

U	
United States (U.S.) and its territorial areas	The 50 states, the District of Columbia (D.C.), 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.
Upgrade	A determination that certain classified information, in the interest of national security, requires a higher degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such a higher degree.

Back to Top

V

Back to Top

W

Back to Top

X

Back to Top

Y

Back to Top

Z

Back to Top