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

Back to Top

A	
Access	The ability and opportunity to gain knowledge of classified information.
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 to 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.
Adverse Information	Any information that adversely reflects on the integrity or character of a cleared employee and suggests that his 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 as an insider threat.
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.

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 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).
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 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.

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" 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) programs or projects which require access to classified information by a contractor.
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 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.
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 a Facility Security Clearance (FCL) by a Cognizant Security Agency (CSA) and is participating in the NISP.
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 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 these agencies when disclosed or released to U.S. industry. Those agencies are the Department of Defense (DOD), Department of Energy (DOE), Office of the Director of National Intelligence (ODNI), and the Nuclear Regulatory Commission (NRC). E.O. 13691 established the Department of Homeland Security (DHS) as a CSA.
Cognizant Security Office (CSO)	The organizational entity delegated by the head of a CSA to administer industrial security on behalf of the CSA.
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	Disclosure of information to unauthorized persons, or a violation of security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

C	
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 (OCA) is able to identify or describe.
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.
Contractor	Any industrial, educational, commercial, or other entity that has been granted an entity eligibility determination by a 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.
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, persons, their agents, or international terrorist organizations.
Critical-sensitive	Any civilian national security position that has the potential to cause exceptionally grave damage to the national security.

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 Under Secretary of Defense for Intelligence and Security provides authority, direction and control over DCSA. DCSA supports national security and 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 PCL process, delivering security education, training and certification, and providing information technology services that support the industrial and personnel security missions of the DOD and its partner agencies. It services over 100 federal entities, oversees over 10,000 cleared companies, and conducts approximately 2 million background investigations each year.
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.

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 also to any successor of the DOD Personnel Security System of Record.
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 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 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, 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 procedures. The term "entity" as 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.

E	
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.
Exclusion Resolutions	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. A determination by the CSA that 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.
Executive Order (E.O.)	A determination by the CSA that 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.
Facility (Security) Clearance (FCL)	An administrative determination that, from a security viewpoint, a company is eligible for access to classified information of a certain category (and all lower categories). FCL is also referred to as an entity eligibility determination.
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 Investigative Standards (FIS)	Standards that apply to investigations that determine eligibility for access to classified information, holding a national security position, physical and logical access, and 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.

F	
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.

Back to Top

G

Back to Top

H	
Homeland Security Presidential Directive 12 (HSPD-12)	The HSPD-12 mandates a federal standard for secure and reliable forms of identification per U.S. policy to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractor employees. The revised FIS established a new investigative model which aligns and standardizes national security background investigation requirements for HSPD-12, suitability and fitness, and national security into five tiers.

Back to Top

I	
Individual Culpability	An individual responsible for a security violation, including evidence of deliberate disregard, gross negligence, and a pattern of negligence or carelessness.
Industrial Security	The 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 complies with the NISP.
Information	Any knowledge that can be communicated or documented, regardless of its physical form or characteristics.
Insider	Cleared contractor personnel with authorized access to any 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 NSI.
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.
Investigation	The action of investigating something or someone; formal or systematic examination or research.

I	
Investigative Service Provider (ISP)	A federal agency or federal contract agency that conducts National Security Background Investigations for the DOD.

Back to Top

J

Back to Top

K	
Key Management Personnel (KMP)	A company's Senior Management Official (SMO), FSO, 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 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 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.
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.
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.

Back to Top

N	
National Industrial Security Program (NISP)	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 32 CFR Part 117, also referred to as the National Industrial Security Program Operating Manual (NISPOM).

N	
National Industrial Security Program Operating Manual (NISPOM) – 32 CFR Part 117	Implements policy, assigns responsibilities, establishes requirements, and provides procedures consistent with E.O. 12829, "National Industrial Security Program;" E.O. 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 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 after 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 (SCI), RD, and controlled or special access program information.
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).
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 to perform tasks or services essential to the fulfillment of a classified contract or program.
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.

Back to Top

O	
Office of the Director of National Intelligence (ODNI)	The USG agency that retains authority over access to intelligence sources and methods. The ODNI is also the USG 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.
Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S))	Responsible for overseeing NISP policy and management.

Back to Top

P	
Personnel Security (PERSEC)	A 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 PCL being granted. PCL is also referred to as national security eligibility determination.
Personnel Security Program (PSP)	The PSP establishes the standards, criteria, and guidelines upon which national security eligibility determinations are based. The PSP uses a comprehensive background investigative process in making this determination. It applies to members of the Armed Forces, DOD civilian employees, DOD contractors, and other affiliated people who require access to classified information or are assigned to sensitive duties. The goal of the program is to ensure the protection of national security.

Back to Top

Q	
Questionnaire for National Security Positions (Security Questionnaire)	The standard form that the DOD uses for most national security background investigations. The form is generally completed electronically via a secure system.

Back to Top

R	
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.

Back to Top

R	
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 CV program, are screened using a risk management-based approach, where an individual's Questionnaire for National Security Positions is analyzed using deferment protocols and is identified for either enrollment in Continuous Evaluation (CE) or submission to an ISP for a reinvestigation.
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 cost in loss of life, dollars, resources, programmatic impact, etc.

Back to Top

S	
Scope	The time period covered and the sources of information 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 national security that the OCA is able to identify or describe.
Security Policy and 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.
Security Training, Education, and Professionalization Portal (STEPP)	The learning management system used by the CDSE. STEPP maintains a list of courses, student information, and course transcripts.
Senior Management Official (SMO)	An U.S. citizen employee occupying a position 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 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 Information/Position	An agency, installation, person, position, document, material, or activity requiring special protection from disclosure, loss, misuse, alteration, or destruction. Breaches could cause embarrassment, compromise, or threat to the security of the sponsoring power and/or adversely affect national security or Governmental interests.
Special Access Program (SAP)	Any program that is established to control access, distribution, and 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-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 DOD or military departments.

S	
Subcontractor	A supplier, distributor, vendor, or firm that furnishes supplies or services to or for a prime contractor or another subcontractor, who enters a contract with a prime contractor. Per NISPOM, each subcontractor will be considered a prime contractor in relation to its subcontractors.
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.

Back to Top

T	
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 could reasonably be expected to cause exceptionally grave damage to national security that the OCA is able to identify or describe.
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; information or data transmitted electronically. 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.

Back to Top

U	
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.
Unfavorable (National Security) Determination	A denial or revocation of eligibility for access to classified information and/or to occupy a sensitive position.
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	
Vetting	A process to review the background of an individual to determine (or who 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 positon.

Back to Top

W	

Back to Top

X	

Back to Top

Y	

Back to Top

Z	

Back to Top