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, 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.
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.
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.

Back to Top

B	
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.
Business Structure	Organization framework legally recognized in a particular jurisdiction for conducting commercial activities such as sole proprietorship, partnership, and corporation.

Back to Top

C	
Center for Development of Security Excellence (CDSE)	A nationally accredited, award-winning directorate within the DCSA. CDSE provides security, training, and certification products and services for the DOD and industry.
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,

C	
	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.
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" also are applicable to all phases of pre-contract activity, including solicitations (bids, quotations, and proposals), pre-contract negotiations, post-contract activity, or other GCA program or project which requires access to classified information by a contractor.
Classified Information	Official information that follows 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 Visit	A visit during which a visitor will require, or is expected to require, access to classified information.
Cleared Contractor (CC)	A facility operating under the National Industrial Security Program (NISP) that has an entity eligibility determination that they are eligible, from a security point of view, for access to classified information of a certain level and all lower levels.
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, Office of the Director of National Intelligence, Department of Energy, and the Nuclear Regulatory Commission. EO 13691 established the Department of Homeland Security 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. For the DOD, DCSA is the CSO.
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

C	
	support a variety of mechanized systems throughout the government.
Communications Security (COMSEC)	Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. government relating to national security and to ensure the authenticity of such communications.
Company	A generic and comprehensive term that may include sole proprietorships, partnerships, corporations, societies, associations, and organizations usually established and operating to carry out a commercial, industrial, or other legitimate business, enterprise, or undertaking.
CONFIDENTIAL	The classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.
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 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)	The 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.
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.
Controlled Unclassified Information (CUI)	Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-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.
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)	DCSA representative who assists Facility Security Officers (FSOs) in identifying potential threats to U.S. technology and developing Counterintelligence (CI) awareness and reporting by company employees.

C	
Critical Nuclear Weapons Design Information (CNWDI)	A DOD category of TOP SECRET RD or SECRET RD that reveals the theory of operation or design of the components of a thermonuclear or fission bomb, warhead, demolition munition, or test device.
Cyber Security	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication including information contained therein, to ensure its availability, integrity, authentication confidentiality and non-repudiation.

Back to Top

D	
Debrief	The process of informing a person their need-to-know for access is terminated.
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 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 Federal Acquisition Regulation Supplement (DFARS)	The 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.
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.
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 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.
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.

D	
Department of Energy (DOE)	The DOE is an executive department of the federal government concerned with the United States' policies regarding energy and safety in handling nuclear material.
Department of Homeland Security (DHS)	The DHS is an executive department of the federal government that was established in response to the aftermath of September 11, 2001. Their primary objective is to protect U.S. citizens and interests from terrorist attacks.

Back to Top

E	
Eligibility	A DOD Consolidated Adjudication facility (DOD CAF) has made an adjudicative determination of person's Personnel Security Investigation (PSI) and that member may 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.
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.
Executive Order (EO)	An order issued by the President to create a policy and regulate its administration within the Executive Branch.

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).

F	
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 NISPOM and any revisions to the manual, notice of which has been furnished to the contractor.
Field Office Chief (FOC)	DCSA representative who manages implementation of NISP and AA&E programs. The FOC ensures that there is effective counterintelligence support to cleared facilities and government contracting activities throughout their area of responsibility. The FOC also oversees the conduct of security reviews by IS Reps. Manages office budget, vehicle utilization, and other property.
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 which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts.

Back to Top

G	
Government Contracting Activity (GCA)	An element of an agency designated by the agency head and delegated broad authority regarding acquisition functions.

Back to Top

H	

Back to Top

I	
Industrial Security	That portion of information security concerned with the protection of classified information in the custody of U.S. industry.

I	
Industrial Security Representative (IS Rep)	DCSA local representative that provides advice and assistance to establish the security program and to ensure a facility is in compliance with the NISP.
Information Security	The system of policies, procedures, and requirements established to follow executive orders, statutes, or regulations 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 Systems	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 Manager (ISSM)	An individual appointed by a contractor with oversight responsibility for the development, implementation, and evaluation of the facility's information system security program. The ISSM must be trained to a level commensurate with the complexity of the facility's information systems.
Information Systems Security Professional/Security Control Assessor (ISSP/SCA)	The ISSP/SCA performs oversight of a contractor's information system processing classified information and provides an authorization decision recommendation to the Authorizing Official (AO).
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 impacts the contractor or agency's obligations to protect classified national security information.
Insider Threat Program Senior Official (ITPSO)	A U.S. citizen employee, appointed by a contractor who establishes and maintains a contractor insider threat program.
Installation Commander	Installation commanders provide installation-specific procedures for work performed on a government installation.
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.

Back to Top

J

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	

Back to Top

M	

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 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 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.
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.
Nuclear Regulatory Commission (NRC)	The NRC was created as an independent agency by Congress in 1974 to ensure the safe use of radioactive materials for beneficial civilian purposes while protecting

N	
	people and the environment. The NRC regulates commercial nuclear power plants and other uses of nuclear materials, such as in nuclear medicine, through licensing, inspection and enforcement of its requirements.

Back to Top

O	
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.

Back to Top

P	
Personally Identifiable Information (PII)	PII refers to 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	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 Specialist	A DCSA representative who conducts inquiries into the activities of an individual, 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.
Prime Contractor	The contractor who receives a prime contract from a GCA.
Program Manager (PM)	Individual with assigned responsibility for maintaining the appropriate operational security posture for a classified contract.

Back to Top

Q	

Back to Top

R	
Request for Proposal (RFP)	A formal negotiated solicitation that results in a formal contract award.

Back to Top

S	
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.
SECRET	The classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to national security.
Security Classification Guidance	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 classified 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 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 Specialist	Also called Activity Security Managers that act as the GCA representatives to the NISP and serve as resident security Subject Matter Experts (SMEs). They also maintain security cognizance over all activity information, personnel, information systems, physical security and industrial security.
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.
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 validate that they not only meet NISPOM requirements but are

S	
	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.
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. A Special Access Program can be created or continued only as authorized by a senior agency official delegated such authority pursuant to the NISPOM.
Standard Form 86 (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.
Statement of Work (SOW)	Designed to describe not only what is to be done but also how it is to be done.
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.
Subject Matter Expert (SME)	An expert in a particular field who contributes or verifies the accuracy of specific information needed by the project team.
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 Report (SCR)	A report of CI concern that likely represents efforts by an individual to obtain illegal or unauthorized access to classified information or technology.

Back to Top

T	
Termination Contracting Officer (TCO)	A TCO will negotiate the terms of termination of an existing contract with a government contractor, if the contract needs be terminated early, whether for convenience or cause.

T	
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.

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.

Back to Top

V	
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).

Back to Top

W

Back to Top

X

Back to Top

Y

Back to Top

Z

Back to Top