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.
Activity	The DOD unit, organization, or installation performing a function or mission.
Activity Address Code (AAC)	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 the DOD for defense agencies.
Alternative Compensatory Control Measures (ACCM) Information	ACCM are security measures used by United States Government (USG) agencies to safeguard classified intelligence or operations when normal measures are insufficient to achieve strict need-to-know controls and where Special Access Program (SAP) controls are not required.

Back to Top

B	

Back to Top

C	
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 Guidance	Instruction or source that prescribes classification of specific information.
Classification Guide	See Security Classification Guide (SCG)
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.

Classified Contract	Any contract, license, agreement, or grant requiring access to classified information by a contractor and its employees for performance. A contract is referred to per the National Industrial Security Program Operating Manual (NISPOM) as a "classified contract" even when the contract document and the contract provisions are not classified. The requirements prescribed for a "classified contract" also are applicable to all phases of pre-contract, license or grant 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 or successor order, and the Atomic Energy Act (AEA) of 1954, as amended, to require protection against unauthorized disclosure in the interest of national security and which has been so designated. The term includes NSI, Restricted Data (RD), and Formerly Restricted Data (FRD).
Cognizant Security Agency (CSA)	Agencies of the Executive Branch that were 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 United States (U.S.) industry. Those agencies are: 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 CSA to administer industrial security on behalf of the CSA.
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, 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 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 (OCA) is able to identify or describe.
Contract Award	Requires completion of final evaluations and approval of the required clearance documentation. The GCA notifies the contractor of the award.

Contracting Officer (CO)	The USG 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 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 CSA. This term also includes licensees, grantees, or certificate holders of the USG with an entity eligibility determination granted by a CSA. As used per NISPOM, "contractor" does not refer to contractor employees or other personnel.
Contracts Manager	Generally responsible for a company's contract management or contract administration of contracts made with customers, vendors, partners, or employees. Contract management includes negotiating the terms and conditions in contracts and ensuring compliance with the terms and conditions, as well as documenting and agreeing on any changes or amendments that may arise during its implementation or execution.
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.
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.
Critical Nuclear Weapons Design Information (CNWDI)	A DOD category of TOP SECRET RD or SECRET RD information that reveals the theory of operation or design of the components of a thermonuclear or fission bomb, warhead, demolition munition, or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited life components; and total contained quantities of fissionable, fusionable, and high explosive materials by type. Among these excluded items

	are the components that DOD personnel set, maintain, operate, test or replace.

Back to Top

D	
DD Form 254 (DOD Contract Security Classification Specification)	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.
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 Sensitive Compartmented Information (SCI).
Defense Federal Acquisition Regulation Supplement (DFARS)	Implements and supplements the Federal Acquisition Regulation (FAR), and is administered by the DOD. The DFARS should be read in conjunction with the primary set of rules in the FAR.
Defense Logistics Agency (DLA)	The DOD's combat logistics support agency. DLA provides the Army, Marine Corps, Navy, Air Force, other federal agencies and partner nation armed forces with a full spectrum of logistics, acquisition, and technical services.
Defense Technical Information Center (DTIC)	The repository for research and engineering information for the DOD. Its suite of services is available to DOD personnel, defense contractors, federal government personnel and contractors, and selected academic institutions. The general public can also access unclassified, unlimited information, including many full-text downloadable documents, through the public DTIC website.
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.
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.

Back to Top

E

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 Clearance (FCL)	An administrative determination that, from a security viewpoint, an entity is eligible for access to classified

F	
	information of a certain level (and all lower levels) (*e.g.*, a type of favorable entity eligibility determination used by some CSAs).
Facility Security Officer (FSO)	The FSO is an 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.
FCL System of Record	The FCL system of record for this course is the National Industrial Security System (NISS). The NISS is a repository of information about DOD cleared contractor facilities. The system has internal users (with full access such as Defense Counterintelligence and Security Agency (DCSA) personnel) and external users (with limited access). The NISS offers a variety of functionality that facilitates the process for FCL requests, processing, and maintenance. Functions and features in NISS include but are not limited to the following: request an FCL, report a change condition, message your Industrial Security Representative (ISR), request a facility profile update, submit an FCL verification and submit an annual self-inspection certification.
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.
Federal Acquisition Regulation (FAR)	The FAR provides uniform policies and procedures for acquisition and identifies the mandatory contract clauses that must be included in a contract document. The FAR also provides guidance on additional clauses for disclosure, protection, and compliance with safeguarding classified and sensitive information.
Follow-On Contract	A GCA or prime contractor awards a follow-on contract to the same contractor or subcontractor for the same item or services as a preceding contract.
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 United States 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.
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

F	
	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.

Back to Top

G	
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.

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.
Information	Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics.
Information Security (INFOSEC)	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 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.
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.
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 Worldwide Intelligence Communications System (JWICS)	A TOP SECRET/SCI network run by the U.S. Defense Intelligence Agency (DIA) and used across the DOD, Department of State (DOS), Department of Homeland Security (DHS) and Deportment of Justice (DOJ) to transmit especially sensitive classified information.

Back to Top

K

Back to Top

L

Back to Top

M

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.
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	On February 24, 2021, Title 32 of the Code of Federal Regulations (CFR) Part 117, NISPOM became effective as a federal rule. Referred to as the "NISPOM rule." The rule 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 CFR 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 Interest Determination (NID)	A written statement by the GCA affirming that the release of proscribed information to a company operating under an Special Security Agreement (SSA) will not harm the national security interests of the U.S.

N	
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.
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 outside of NATO.

Back to Top

O	
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.

Back to Top

P	
Prime Contract	A contract awarded by a GCA to a contractor for a legitimate USG purpose.
Prime Contractor	The contractor who receives a prime contract from a GCA.
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 Manager (PM)	The designated individual responsible for a program and manages all daily aspects of it.

Back to Top

Q

Back to Top

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

R	
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.
Restricted Data (RD)	All data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) 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 AEA.

Back to Top

S	
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.
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 and prescribes the level and duration of classification and appropriate declassification instructions.
Security Specialists	Also called Activity Security Managers that act as GCA representatives to the NISP and serve as a resident security Subject Matter Expert (SME). They also maintain security cognizance over all activity information, personnel, information systems, physical security and industrial security.
Sensitive Compartmented Information (SCI)	A subset of Classified National Intelligence concerning or derived from intelligence sources, methods, or analytical processes, that is required to be protected within formal access control systems established by the Director of National Intelligence.
Solicitation	Any request to submit offers or quotations to the government. Solicitations under sealed bid procedures are called IFB. Solicitations under negotiated procedures are called RFP. Solicitations under simplified acquisition procedures may require submission of either a quotation or an offer. Solicitations are used in negotiated procurement to communicate government requirements to the contractor.
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

S	
	CONFIDENTIAL information. A SAP can be created or continued only as authorized by a senior agency official delegated such authority pursuant to E.O. 13526.
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, RFP, 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. Per NISPOM, each subcontractor will be considered as a prime contractor in relation to its subcontractors.
Subject Matter Expert (SME)	An expert in a particular field who contributes or verifies the accuracy of specific information needed by the project team.

Back to Top

T	
TEMPEST	The protection of sensitive information being compromised from electronic equipment producing emissions, including unintentional radio, or electrical signals, sounds, and vibrations.
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.

Back to Top

U	
United States Transportation Command (USTRANSCOM)	Provides air, land, and sea transportation for the DOD in times of peace and war. It moves people and property around the world.

Back to Top

V

Back to Top

W

Back to Top

X

Back to Top

Y

Back to Top

Z

Back to Top