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 the Department of Defense (DOD) needs, intended for use in, or in support of, military missions.
Acquisition Framework	The management process by which the DOD provides effective, affordable, and timely systems to the users. It consists of phases containing major activities and associated decision points, during which a system goes through research, development, test, and evaluation (RDT&E); production; fielding or deployment; sustainment; and disposal.
Acquisition Program	A directed, funded effort that provides a new, improved, or continuing materiel, weapon, or information system or service capability in response to an approved need. Acquisition programs are divided into categories that are established to facilitate decentralized decision making, execution, and compliance with statutory requirements.
Analysis of Alternatives (AoA)	Assessment of potential materiel solutions to satisfy the capability need documented in the approved Initial Capabilities Document (ICD). It focuses on identification and analysis of alternatives, Measures of Effectiveness (MOE), cost, schedule, concepts of operations, and overall risk, including the sensitivity of each alternative to possible changes in key assumptions or variables.
Analysis of Alternatives (AoA) Study Plan	Based on the AoA Study Guidance, the AoA Study Plan establishes a roadmap of how the analysis must proceed, who is responsible for the different elements, and why they are doing them. The Study Plan is a "living document" and must be updated throughout the AoA effort to reflect new information and changing study perceptions and direction.

Back to Top

B

Back to Top

C	
Capability Design Document (CDD)	A CDD (includes the Information System (IS) CDD variant) specifies capability requirements in terms of developmental Key Performance Parameters (KPP), Key System Attributes (KSA), Additional Performance Attributes (APA), and other related information necessary to support development of one or more increments of a materiel capability solution.
Center for Development of Security Excellence (CDSE)	A nationally accredited, award-winning directorate within the Defense Counterintelligence and Security Agency (DCSA). The CDSE is the premier provider of security training, education, and certification for the DOD, Federal Government, and industry under the National Industrial Security Program (NISP). The CDSE provides development, delivery, and exchange of security knowledge to ensure a high-performing workforce capable of addressing our Nation's security challenges.

C	
Certificate Pertaining to Foreign Interests (SF 328)	A survey with questions designed to help identify the presence of Foreign Ownership, Control, or Influence (FOCI) in an organization, and provides the basis around which the FOCI analysis process is organized. The form is completed using the Facility Clearance (FCL) system of record
Classification Management	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 United States (U.S.) government.
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 Government Contracting Activity (GCA) program or project which requires 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).
Cleared Contractors	A person or facility operating under the NISP that has had an administrative determination that they are eligible, from a security point of view, for access to classified information of a certain level and all lower levels.
Cognizant Security Agencies (CSA's)	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. These agencies are: DOD, Office of the Director of National Intelligence (ODNI), Department of Energy (DOE), 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.
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.
Communications Security (COMSEC)	Defined as the protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. government concerning national security, and to ensure the authenticity of such telecommunications.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Contract Award	The process of formally notifying a company that they have been selected to perform work and/or provide services on a particular government contract. Requires completion of final proposal evaluations and eligibility. Approval occurs when the government Contracting Officer (CO) has signed and distributed the contract to the contractor.

C	
Contract Closeout	During this phase the CO must ensure that the work conforms to the requirements in the Statement of Work (SOW) or Performance Work Statement (PWS). Any deficiencies must be resolved before final payment is made. Unless retention is approved by the government, all classified material must be returned to the GCA or destroyed.
Contract Management	In the Contract Management phase, the contractor provides the agreed-upon product or service. The GCA works with the Facility Security Officer (FSO) to monitor and mitigate threats and vulnerabilities.
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 classified contract.
Contracting Officer	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 their authority.
Contracting Officer's Representative (COR)	Determines the need for contractor access to classified information, verifies the FCL, and communicates the security requirements during the procurement process and contract performance to the contractor.
Contractor	Any industrial, educational, commercial, or other entity that has been granted an entity eligibility determination, also referred to as an FCL, by a CSA. This term also includes licensees, grantees, or certificate holders of the United States Government with an FCL granted by a CSA. As used in the National Industrial Security Program Operating Manual (NISPOM), ''contractor'' does not refer to contractor employees or other personnel.
Cooperative Research and Development Agreement (CRADA)	A CRADA authorizes federal labs to enter into agreements with other federal agencies, state/local government, industry, non-profits, and universities for licensing agreements for lab developed inventions or intellectual property to commercialize products or processes originating in federal labs.
Critical Program Information (CPI)	Elements or components of a Research, Development, and Acquisition (RDA) program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability.
Criticality Analysis (CA)	Procedure by which each potential failure mode is ranked according to the combined influence of severity and probability of occurrence.

Back to Top

D	
Defense Counterintelligence and Security Agency (DCSA)	DCSA protects America's trusted workforce, trusted workspaces, and classified information. To do so, they have two fundamental missions: personnel security and industrial security. Supporting these two core missions are counterintelligence and insider threat and security training. The DCSA is the largest investigative provider in the federal government and oversees cleared facilities under the NISP. They reply on the Personnel and Industrial Security, Counterintelligence and Insider Threat directorates

D	
	to ensure the security of the nation's technologies and information. The agency is also comprised of nationally accredited training centers that provide security training, education, and certifications for security professionals.
Defense Counterintelligence and Security Agency, Industrial Security Representative (IS Rep)	Local representative from the DCSA that provides advice and assistance to establish the security program and to ensure a facility is in compliance with the NISP.
Defense Counterintelligence and Security Agency, Information Systems Security Professional (ISSP)	Local representative from the DCSA that performs oversight of a contractor's information system processing classified information and provides an authorization decision recommendation to the Authorizing Official (AO).
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 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, contractors, and selected academic institutions. The general public can also access unclassified, unlimited information, including many full-text downloadable documents, through the public DTIC web site.
Department of Defense (DOD)	The largest CSA, 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. The DOD's enduring mission is to provide combat-credible military forces needed to deter war and protect the security of our nation.
Department of Defense Security Agreement (DD Form 441)	A DOD Security Agreement between a contractor who will have access to classified information and the DOD in order to preserve and maintain the security of the U.S. through the prevention of unauthorized disclosure of classified information.
Department of Defense Registration for Scientific and Technical Information Services (DOD Form 1540)	Used to validate an individual's required affiliation with a DOD organization.
Department of Defense Security Specialist	Acts as the GCA representatives to the NISP and serve as resident security Subject Matter Experts (SME). They also maintain security cognizance over all activity information, personnel, information systems, physical security and industrial security.
Development RFP Release Decision	The point at which planning for development is complete and a decision is made to release a Request for Proposal (RFP).
Disposal	At the end of its useful life, a system will be demilitarized and disposed of in accordance with all legal and regulatory requirements and policy relating to safety (including explosives safety), security, and the environment.

Back to Top

E	
Eligibility	The DCSA 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.
Engineering & Manufacturing Development (EMD)	The purpose of the EMD phase is to develop, build, test, and evaluate a materiel solution to verify that all operational and implied requirements,

E	
	including those for security, have been met, and to support production, deployment and sustainment decisions. During the EMD phase, a contract is awarded to demonstrate an affordable, supportable, interoperable, and producible system in its intended environment.
Executive Order (EO)	An order issued by the President of the U.S. to create a policy and regulate

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). An 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 related security requirements to ensure the protection of classified information. The FSO must complete security training per the NISPOM and possess a national security eligibility determination, also referred to as a Personnel Security Clearance (PCL), at the same level as the facility's FCL.
Federal Acquisition Regulation (FAR)	The 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 DOD Security Agreement (DD Form 441), the NISPOM, and any applicable revisions.
Foreign Government Information (FGI)	Information that is provided to the U.S. by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or produced by the U.S. pursuant to, or as a result of, a joint arrangement with a foreign government or governments, an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence.
Foreign Interest	Any 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 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, to direct or decide matters affecting the management or operations of a company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts.
Full Rate Production	The second effort part of the Production and Deployment (P&D) phase as defined and established by DoDI 5000.02 after Low-Rate Initial Production (LRIP) and following a successful Full-Rate Production Decision Review (FRPDR).

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.
Industrial Security Letters (ISL)	Documents that provide detailed operational guidance and notification of changes to or clarification of existing policies or requirements to the NISPOM.
Information Security	The system of policies, procedures, and requirements established pursuant to executive order, statute, or regulation to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security. The term also applies to policies, procedures, and requirements established to protect unclassified information that may be withheld from release to the public.
Information System Security Manager (ISSM)	An individual appointed by a contractor with oversight responsibility for the development, implementation, and evaluation of the facility's classified information system program. The ISSM must be trained and possess technical competence commensurate with the complexity of the facility's classified information systems. The ISSM must be eligible for access to classified information to the highest level of the information processed on the system(s) under their responsibility.
Information System Security Officer (ISSO)	Assigned by the ISSM when the facility has multiple authorized Information Systems (IS) in multiple facility organizations in which the ISSM has oversight responsibility for the multiple facilities, or when the technical complexity of the facility's IS program warrants the appointment.
Initial Capabilities Document (ICD)	Documents one or more new capability requirements and associated capability gaps. The ICD also documents the intent to partially or wholly address identified capability gap(s) with a non-materiel solution, materiel solution, or some combination of the two.
Initial Operational Test and Evaluation (IOT&E)	Dedicated Operational Test and Evaluation (OT&E) conducted on production or production representative articles, to determine whether systems are operationally effective and suitable to support a Full-Rate Production (FRP) decision. The term IOT&E is normally associated with programs on the Director, OT&E oversight list.

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

K	
	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.
Key Performance Parameters (KPP)	Performance attribute of a system considered critical or essential to the development of an effective military capability. KPPs are contained in the Capability Development Document (CDD) and the Capability Production Document (CPD) and are included verbatim in the Acquisition Program Baseline (APB).
Key System Attributes (KSA)	Performance attribute of a system considered important to achieving a balanced solution/approach to a system, but not critical enough to be designated as a KPP. KSAs must be measurable, testable, and support efficient and effective Test and Evaluation (T&E).

Back to Top

L	
Lowest Price and Technically Acceptable (LPTA)	Source selection process appropriate when best value is expected to result from selection of a technically acceptable proposal with the lowest evaluated price.
Low-Rate Initial Production (LRIP)	The first part of the Production and Deployment (P&D) phase. LRIP is intended to result in completion of manufacturing development in order to ensure adequate and efficient manufacturing capability and to produce the minimum quantity necessary to provide production or production-representative articles for Initial Operational Test and Evaluation (IOT&E).

Back to Top

M	
Materiel Development Decision (MDD)	A review that is the formal entry point into the acquisition process and is mandatory for all programs. A successful MDD may approve entry into the acquisition management system at any point consistent with phase-specific and statutory requirements but will normally be followed by a Materiel Solution Analysis (MSA) phase.
Materiel Solution Analysis (MSA)	Conducts the analysis and other activities needed to choose the concept for the product that will be acquired. At the end of the MSA phase an investment decision is made to pursue specific product or design concepts and to commit the necessary resources.
Milestone (MS)	In the context of scheduling, a specific definable accomplishment in the contract network that is recognizable at a particular point in time.
Milestone Decision Authority (MDA)	Designated individual with overall responsibility for a program. The MDA shall have the authority to approve entry of an acquisition program into the next phase of the acquisition process and shall be accountable for cost, schedule, and performance reporting to higher authority, including congressional reporting.

Back to Top

N	
North Atlantic Treaty Organization (NATO)	NATO is a group of 32 countries from Europe and North America that exists to protect the people and territory of its members. NATO constitutes a system of collective defense whereby its member states agree to mutual defense in response to an attack by any external party.
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

N	
	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)	Implements policy, assigns responsibilities, establishes requirements, and 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 Interest Determination (NID)	A written statement by the GC affirming that the release of proscribed information to the company will not harm the National Security interests of the U.S.
NISP Contract Classification System (NCCS)	NCCS is the enterprise Federal information system application supporting DOD, other Federal Agencies, and cleared industry in the NISP by facilitating the processing and distribution of contract security classification specifications (DD Form 254) for contracts requiring access to classified information.

Back to Top

O	
Operations & Support (O&S)	Phase that executes the product support strategy, satisfies materiel readiness and operational support performance requirements, and sustains the system over its life cycle (to include disposal). Concerns center on sustainment of the fielded system as well as disposal at end-of-life.
Original Classification Authority (OCA)	An individual authorized in writing, either by the U.S. President, the Vice President, agency heads or other officials designated by the President, to classify information in the first instance. OCAs must receive training to perform this duty.

Back to Top

P	
Performance Work Statement (PWS)	States the work in terms of outcomes or results, rather than methods of performance. It defines measurable performance standards and financial incentives.
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. A PCL is also referred to as a national security eligibility determination.
Physical Configuration Audit (PCA)	Physical examination of the actual configuration of the item being produced. It verifies that the related design documentation matches the item as specified in the contract. The system product baseline if finalized and validated at the PCA.
Post-Award	During this phase, the government and the contractor meet and prepare to implement the contract. The program stakeholders come together to review the contract performance requirements and security issues.
Pre-Award	During this phase acquisition planning, issuing the solicitation, and source selection occur. The solicitation is released with the FAR Security Requirements Clause for classified contracts.

P	
Pre-Award Objective	To award the contract to the proposal that represents the best value to the Government.
Pre-Solicitation	Discusses technical and other problems connected with a proposed procurement.
Pre-System Acquisition	Participation in contract preparation and source selection to ensure security concerns are addressed and included in proposals, source evaluations and contract negotiations and cost discussions and performs an initial Criticality Analysis (CA) based on mission threats and system functions.
Prime Contractor	The contractor who receives a prime contract from a GCA.
Privity of Contract	A contract awarded by a GCA to a contractor for a legitimate U.S. Government purpose.
Production and Deployment (P&D)	During the P&D phase, activities focus on achieving Full Operational Capability and ensure any new threat environments are considered.
Program Manager (PM)	Individual with assigned responsibility for maintaining the appropriate operational security posture for a classified contract

Back to Top

Q	
Quality Assurance Surveillance Plan (QASP)	The document government personnel use to assess contractor performance. The QASP identifies what is going to be inspected, the inspection process, and who will do the inspecting.

Back to Top

R	
Request for Proposal (RFP)	A formal negotiated solicitation that results in a formal contract award.
Request for Quote (RFQ)	A solicitation used in negotiated acquisition to communicate government requirements to prospective contractors and to solicit a quotation. A response to an RFQ is not an offer; however, it is informational in character.
Research and Development (R&D)	Includes all scientific study and experimentation directed toward increasing knowledge and understanding in those fields of the physical, engineering, environmental, and life sciences related to long-term national security needs.
Restricted Data (RD)	All data concerning design, manufacture, or utilization of atomic weapons. The production of special nuclear material; or the use of special nuclear material in the production of energy but does not include data declassified or removed from the RD category pursuant to section 142 of the Atomic Energy Act (AEA) of 1954.

Back to Top

S	
Security Training Education and Professionalization Portal (STEPP)	The learning management system used by the CDSE. STEPP is where the list of courses, student information, and course transcripts are maintained.
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 ODNI.
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 RFPs. Solicitations under simplified acquisition procedures may require submission of either a quotation or an offer.

S	
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 SAP can be created or continued only as authorized by a senior agency official delegated such authority pursuant to E.O. 13526.
Statement of Work (SOW)	Designed to describe not only what is to be done, but also how it is to be done.
Subject Matter Expert (SME)	An expert in a particular field who contributes or verifies the accuracy of specific information needed by the project team.
Sustainment	Programs with Critical Program Information (CPI) require continued evaluation and monitoring as protection and threat/vulnerability/countermeasures may have to continue to evolve.
System Acquisition	Updates criticality assessment, risk, threat and mitigation as required and ensure all Critical Program Information (CPI) and mission-critical functions are identified and associated countermeasures applied.
System Functional Review (SFR)	A multi-disciplined technical review to ensure that the system's functional baseline is established and has a reasonable expectation of satisfying the requirements of the Initial Capabilities Document (ICD) or draft Capability Development Document (CDD) within the currently allocated budget and schedule. It completes the process of defining the items or elements below system level.
Systems Security Engineering (SSE)	Performed by a variety of professionals from government and industry to ensure a comprehensive analysis of system technology, hardware, software, firmware, and information.

Back to Top

T	
Technology Maturation & Risk Reduction (TMRR)	During the TMRR phase, the Capability Development Document (CDD) is approved with system-specific requirements, the RFP is released to industry, and technical design and analyses begins.
Test and Evaluation (T&E)	Process by which a system or components are exercised and results analyzed to provide performance-related information. The information has many uses including risk identification and risk mitigation and empirical data to validate models and simulations.
Trade-off	Source selection process allows for a tradeoff between non-cost factors and cost/price and allows the Government to accept other than the lowest priced proposal or other than the highest technically rated proposal to achieve a best-value contract award.

Back to Top

U

Back to Top

V

Back to Top

W

Back to Top

X

Back to Top

Y

Back to Top

Z

Back to Top