A	
Access	The ability and opportunity to gain knowledge of classified information.
Activity	A Department of Defense (DOD) unit, organization, or installation performing a function or mission.
Approved Methods	Maintenance and Repairs of Approved General Services Administration (GSA) Security Containers: Approved methods of maintenance to GSA-approved security containers must be performed as recommended by the manufacturer to retain security integrity and safe operability. When upgrades or modifications are required to sustain the GSA approval status for the protection of classified information, as required per national policy documents, only alterations/modifications authorized by the GSA will be accomplished. Approved methods of repair to a GSA-approved security container is when the repaired GSA-approved security container is restored to its original state of security integrity and meets the conditions specified in the Federal Standard 809, Inspection, Maintenance, Neutralization, and Repair of GSA Approved Containers and Vault Doors. Destruction of Classified Information: Approved methods of classified information identified for destruction shall be destroyed completely to preclude recognition or reconstruction of the classified information. The methods and equipment used to routinely destroy classified information include burning, cross-cut shredding, wet-pulping, melting, mutilation, chemical decomposition, pulverizing, overwriting, degaussing, sanding, or grinding.
Approved Security Container	An approved security container is a GSA-approved security container, the only type of security container that may be used to safeguard classified information. A GSA-approved security container is a steel file container with a built-in combination lock constructed to withstand certain hazards, such as lock manipulation, for specified lengths of time. The security containers bear the GSA approval label on the front face of the container, which identifies them as meeting the applicable testing requirements per the Federal Standard 809, Neutralization and Repair of GSA Approved Containers and Vault Doors. The GSA establishes and publishes uniform standards, specifications, and supply schedules for its approved security containers. All GSA-approved security containers must be procured through the GSA Global Supply System.
Approved Vault	A vault built to Federal Standard 832, Construction Methods and Materials for Vaults, and must be approved by the Cognizant Security Agency (CSA).

A	
Authorized Person	A person who has a favorable determination of eligibility, also referred to as a personnel clearance (PCL), for access to classified information, has signed an approved non-disclosure agreement (NDA), and has a need-to-know (NTK) for the classified information in performance of official duties.

Back to Top

B

Back to Top

C	
Center for Development of Security Excellence (CDSE)	A nationally accredited, award-winning directorate within the Defense Counterintelligence and Security Agency (DCSA). CDSE provides security education, training, and certification products and services to a broad audience supporting the protection of National Security and professionalization of the DOD security enterprise.
Central Office of Record (COR)	The COR provides oversight and guidance to established Communications Security (COMSEC) programs within the COMSEC Material Control System and ensures compliance with national policy.
Certificate Pertaining to Foreign Interest (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 system of record for facility clearance (FCL) information.
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.
Classification-pending	Documents that require a classification determination from the Government Contracting Activity (GCA).

C	
Classified Contract	Any contract requiring access to classified information by a contractor and its employees in the performance of the contract (a contract may be a classified contract even though the contract document is not classified). The requirements prescribed for a "classified contract" also are applicable to all phases of pre-contract activity, including solicitations (bids, quotations, and proposals), pre-contract negotiations, post-contract activity, or other GCA program or project which requires access to classified information by a contractor.
Classified Information	Official information that has been determined, pursuant to Executive Order (E.O.) 13526, Classified National Security Information, or any predecessor order to require protection against unauthorized disclosure in the interest of national security, which has been designated. 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 United States (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.
Clearance	Formal security determination by an authorized adjudicative office that an individual has authorized access, on a need-to-know (NTK) basis, to a specific level of collateral classified information (TOP SECRET, SECRET, or CONFIDENTIAL).
Cleared Employees	All employees of industrial or commercial contractors, licensees, certificate holders, or grantees of an agency, as well as all employees of subcontractors and personal services contractor personnel, and who are granted favorable eligibility determinations for access to classified information by a Cognizant Security Agency (CSA) or are being processed for eligibility determinations for access to classified information by a CSA. A contractor may give an employee access to classified information in accordance with the applicable provisions of the National Industrial Security Program Operating Manual (NISPOM).
Cognizant Security Agency (CSA)	An agency designated as having National Industrial Security Program (NISP) implementation and security responsibilities for its own agencies (including component agencies) and any entities and non-CSA agencies under its cognizance. These agencies are the DOD, Department of Energy (DOE), Office of the Director of National Intelligence (ODNI), Nuclear Regulatory Commission (NRC), and Department of Homeland Security (DHS).

C	
Commercial Delivery Entity	A contractor approved by the CSA that transmits SECRET or CONFIDENTIAL information within the U.S. and its territorial areas that is a current holder of the GSA contract for overnight delivery and provides nation-wide, overnight service with computer tracking and reporting features. The entity does not need to be determined eligible for access to classified information.
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 classified information.
CONFIDENTIAL	The classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.
Contractor	Any industrial, educational, commercial, or other entity that has been granted an entity eligibility determination, also referred to as a facility clearance (FCL) by a CSA. This term also includes licensees, grantees, or certificate holders of the U.S. Government with an FCL granted by a CSA.
Counterintelligence (CI)	Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.
Custodian	An individual who has possession of, or is otherwise charged with, the responsibility for safeguarding classified information.

Back to Top

D	
Declassification	A date or event that coincides with the lapse of the information's national security sensitivity as determined by the original classification authority (OCA). Declassification occurs when the OCA determines that the classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure and the information has had its classification designation removed or cancelled.

D	
Defense Counterintelligence and Security Agency (DCSA)	DCSA is the security agency in the Federal Government dedicated to protecting America's trusted workforce and trusted workspaces — real or virtual. DCSA joins two essential missions: Personnel Vetting and Critical Technology Protection, supported by Counterintelligence and Training, Education, and Certification functions. DCSA services over 100 federal entities, oversees 10,000 cleared companies, and conducts approximately 2 million background investigations each year.
Department of Defense (DOD)	The DOD is the largest U.S. Government agency and provides the military forces needed to deter war and ensure the Nation's security. The DOD has over 10 combatant commands, each with a geographic or functional mission that provides command and control of military forces in peace and war. The Army, Marine Corps, Navy, Air Force, Space Force, and Coast Guard are the armed forces of the U.S. The Army National Guard and the Air National Guard are reserve components of their service and operate in part under state authority.
Derivative Classification	The incorporating, paraphrasing, restating, or generating in new form information that is already classified and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.
Document	Any recorded information, regardless of the nature of the medium or the method or circumstances of recording.
DOD 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.
DOD Personnel Security System of Record	A system of record that serves as the enterprise-wide solution for personnel security, suitability, and credentialing management for DOD military, civilian, and contractors. An innovative, web-based application, the platform provides secure communications between adjudicators, security officers, and components, allowing users to request, record, document, and identify personnel security actions.
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, Access to Classified Information.

Back to Top

E	
Electronic Processing	The capture, storage, manipulation, reproduction, or transmission of data in all forms by any electronically powered device. This definition includes, but is not limited to, computers and their peripheral equipment, word processors, office equipment, telecommunications equipment, facsimiles, and electronic accounting machines, etc.
Eligibility	The DCSA Consolidated Adjudication Services (DCSA CAS) has made an adjudicative determination of a person's personnel security investigation (PSI). That person will have access to classified information equal to the level of their adjudicated investigation.
Eligibility Determination	The decision to grant eligibility for access to classified information or performance of national security duties.
Employee	A person, other than the President and Vice President of the U.S., employed by, detailed, or assigned to an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head.
Escort	An authorized person designated by the contractor who is responsible to brief a visitor on the facility security procedures and accompany the visitor or keep the visitor under visual observation at all times while in the facility or applicable areas to prevent the unauthorized disclosure of classified information and/or to ensure that the visitor only has access to information consistent with the authorized purpose of the visit.
Evaluated Products List (EPL)	The EPL provides equipment that meets National Security Agency specifications. The lists apply to all National Security Agency/Central Security Service (NSA/CSS) elements, contractors, and personnel and pertains to all information systems storage devices that they use.

Back to Top

F	
Facility	A plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components that, when related by function and location, form an operating entity.

F	
Facility (Security) Clearance (FCL)	An administrative determination that, from a security point of view, a company is eligible for access to classified information of a certain category (and all lower categories). FCL is also referred to as an entity eligibility determination.
Facility Security Officer (FSO)	A U.S. citizen employee appointed by a contractor who will supervise and direct security measures necessary for implementing the NISPOM and other Federal requirements for classified information.
Foreign Person	Any foreign national, foreign government, or foreign entity; or any entity over which control is exercised or exercisable by a foreign person.
Foreign Visit	A foreign national enters or proposes to enter a DOD component or cleared contractor facility or to meet with employees or representatives of the facility.

Back to Top

G	
General Services Administration (GSA)	The GSA provides workplaces by constructing, managing, and preserving government buildings and by leasing and managing commercial real estate. GSA's acquisition solutions offer private sector professional services, equipment, supplies, and IT to government organizations and the military. GSA also promotes management best practices and efficient government operations through the development of government-wide policies.
GSA Global Supply System	A federal program administered by the GSA. It is a requisition-based supply program for customers worldwide, including the DOD. Customers can use a variety of ordering mechanisms to submit requisitions to GSA for delivery globally. All GSA-approved security containers must be procured through the GSA Global Supply System.
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	
Home Office	The headquarters of a multiple facility organization (MFO).

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)	Local representative from the DCSA that provides advice and assistance to establish the security program and to ensure a facility is in compliance with the NISP.
Information	Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics.
Information Management System (IMS)	A system to protect and control classified information as required by the NISPOM. The IMS must be capable of facilitating retrieval and disposition of classified material in a reasonable period of time.
Information System	An assembly of computer hardware, software, and firmware configured for the purpose of automating the functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating, or otherwise manipulating data, information, and textual material.
Information System Security Professional/Security Control Assessor (ISSP/SCA)	An employee of DCSA that performs oversight of a contractor's information system processing classified information and provides an authorization decision recommendation to the Authorizing Official (AO).
Intrusion Detection System (IDS)	A security system that is designed to detect a change in the environment and transmit some type of alarm notification.
Investigation	The action of investigating something or someone; formal or systematic examination or research.

Back to Top

J	

Back to Top

K	

Back to Top

L	
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.
Media	Physical devices or writing surfaces including but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

M	
Multiple Facility Organization (MFO)	A legal entity (single proprietorship, partnership, association, trust, or corporation) composed of two or more contractors.

Back to Top

N	
National Industrial Security Program (NISP)	Established by Executive Order 12829, National Industrial Security Program (NISP), 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 Code of Federal Regulations (CFR) Part 117, also referred to as the NISPOM.
National Industrial Security Program Operating Manual (NISPOM)	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 CFR Part 2004, National Industrial Security Program. This 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	The national defense of foreign relations of the U.S. national security, including defense against transnational terrorism.
National Security Agency/Central Security Service (NSA/CSS)	The NSA/CSS leads the U.S. Government in cryptology that encompasses both signals intelligence (SIGINT) insights and cybersecurity products and services and enables computer network operations to gain a decisive advantage for our Nation and allies.
National Security Information (NSI)	Information that follows E.O. 13526, Classified National Security Information, requires protection against unauthorized disclosure and is so marked when in documentary form.
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-Working Hours (Non-WH)	Non-WH includes any time of day when cleared employees are not in the work area; a work force not working on a regularly scheduled shift.
North Atlantic Treaty Organization (NATO)	Information bearing NATO markings, indicating the information is the property of NATO and access to which is limited to representatives of NATO and its member

N	
	nations unless NATO authority has been obtained to release it outside of NATO.

Back to Top

O	
Open Storage Area	An area that meets the requirements of the NISPOM for safeguarding classified material that, because of its size, nature, or operational necessity, cannot be adequately protected by the normal safeguards or stored during non-working hours in approved security containers.
Original Classification	An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure. Only U.S. Government officials who have received designation in writing may apply an original classification to information.
Original Classification Authority (OCA)	An individual authorized in writing by the President, the Vice President, agency heads, or other officials designated by the President to classify information in the first instance.

Back to Top

P	
Parent	An entity that owns a majority of another entity's voting securities.
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.
Perimeter Controls	Perimeter controls are entry and exit inspections that deter and detect the introduction or removal of classified information from a facility without proper authority.
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 a national security eligibility determination.
Personnel Security	A security discipline that assesses the loyalty, reliability, and trustworthiness of individuals for initial and continued eligibility for access to classified information.
Physical Security	The security discipline concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.
Prime Contract	A contract awarded by a GCA to a contractor for a legitimate U.S. Government purpose.
Prime Contractor	The contractor who receives a prime contract from a GCA.

Back to Top

Q

Back to Top

R	
Receipt	A written or digitally signed acknowledgment of having received a specified item, information, freight, or documents.
Restricted Area	A controlled access area established to safeguard classified material that because of its size or nature cannot be adequately protected during working hours by the usual safeguards but that is capable of being stored during non-working hours in an approved repository or secured by other methods approved by the CSA.
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	
SECRET	The classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.
Security Clearance	A national security eligibility determination by competent authority that an individual is eligible for access to NSI, under the standards of the NISPOM. Also called a clearance. The individual must have both eligibility and access to have a security clearance. Eligibility is granted by the adjudication facilities, and the access is granted by the individual agencies.
Security-in-depth	A determination made by the CSA that a contractor's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within a facility. Examples include, but are not limited to, use of perimeter fences, employee and visitor access controls, use of an IDS, random guard patrols throughout the facility during non-working hours, closed circuit video monitoring, or other safeguards that mitigate the vulnerability of open storage areas without alarms and security storage cabinets during non-working hours. Written authorization from the CSA is required before security-in-depth can take the place of supplemental controls.
Security Training Education and Professionalization Portal (STEPP)	The learning management system used by CDSE. STEPP maintains a list of courses, student information, and course transcripts.

S	
Standard Practice 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.
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, Request For Quotation (RFQ), Request for Proposal (RFP), Invitation For Bid (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 furnishes supplies or services to or for a prime contractor or another subcontractor who enters into a contract with a prime contractor. Per the NISPOM, each subcontractor will be considered as a prime contractor in relation to its subcontractors.
Subsidiary	An entity in which another entity owns a majority of its voting securities.
Supplemental Protection	An IDS meeting the requirements stated in the NISPOM. NOTE: Security Guards may continue to be used as supplemental protection only if approved prior to January 1, 1995.
System Security Plan (SSP)	A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

Back to Top

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 that the original classification authority 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. 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 Access	A person not authorized to have access to specific classified information in accordance with the requirements of the NISPOM.

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.
Unauthorized Person/Personnel	A person not authorized to have access to specific classified information in accordance with the requirements in the NISPOM.

Back to Top

V

Back to Top

W	
Working Hours (WH)	The period of time when: 1. There are employees present in the specific area where classified material is located, a work force on a regularly scheduled shift, as contrasted with employees working within an area on an overtime basis outside of the scheduled work shift. 2. The number of employees in the scheduled work force is sufficient in number and so positioned to be able to detect and challenge the presence of unauthorized personnel. This would, therefore, exclude janitors, maintenance personnel, and other individuals whose duties require movement throughout the facility.
Working Papers	Documents or materials, regardless of the media, which are expected to be revised prior to the preparation of a finished product for dissemination or retention.

Back to Top

X

Back to Top

Y

Back to Top

Z

Back to Top