A	
Access	The ability and opportunity to gain knowledge of classified information.

Back to Top

B	

Back to Top

C	
Center for Development of Security Excellence (CDSE)	A nationally accredited, award-winning directorate within the DCSA. The CDSE is the premier provider of security training, education, and certification for the DOD, federal government, and cleared contractors under the National Industrial Security Program (NISP)
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 Facility Clearance (FCL) system of record.
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 Guide	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.
Classified Contract	Any contract requiring access to classified information by a contractor or his or her employees in the performance of the contract. (A contract may be a classified contract even through 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/Material	Information that has been determined pursuant to Executive Order (E.O.) 13526 or any predecessor order to require protection against unauthorized disclosure in the interest of national security. The term includes NSI, Restricted Data (RD), and Formerly Restricted Data (FRD).
Classified Visit	A visit during which a visitor will require, or is expected to require, access to classified information.

C	
Classified Working Papers	Documents that are generated in the preparation of a finished classified document and must be safeguarded.
Cleared Employees	All industrial or commercial contractors, licensees, certificate holders, or grantees of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head who are granted Personnel Security Clearances (PCL) or are being processed for PCLs.
Cognizant Security Agencies (CSAs)	Agencies of the Executive Branch that have been authorized by Executive Order 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: The Department of Defense, Department of Energy, Office of the Director of National Intelligence, Nuclear Regulatory Commission, and Department of Homeland Security.
Cognizant Security Office (CSO)	The organizational entity delegated by the head of a CSA to administer industrial security on behalf of the CSA.
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.
CONFIDENTIAL	The classification level applied to information, the unauthorized disclosure of which reasonable could be expected to cause damage to the national security that the original classification authority is able to identify or describe.
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.
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 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.

Back to Top

D	
Data Spill	Known also as contaminations or classified message incidents, occurs when classified data or controlled unclassified information (CUI) is introduced to an unclassified computer system or to a computer system accredited at a lower classification level than the data being entered.
DD Form 441 (Security Agreement)	A Department of Defense Security Agreement that is entered into 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.
DD Form 441-1	The appendage to the DOD Security Agreement and lists—if applicable—cleared divisions or branches included in and covered by the provisions of the organization's DOD Security Agreement (DD Form 441) and Certificate Pertaining to Foreign Interest (SF 328).
Debriefing	The process of informing a person their need-to-know for access is terminated.
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.
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.
DOD Personnel Security System of Record	A system of record for personnel security, adjudication determination, clearance, verification, and history.

Back to Top

E	
Eligibility	The DOD Consolidated Adjudication Services (DOD 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.
Entity	A generic and comprehensive term which may include sole proprietorships, partnerships, corporations, limited

E	
	liability companies, societies, associations, institutions, contractors, licensees, grantees, certificate holders, and other organizations usually established and operating to carry out a commercial, industrial, educational, or other legitimate business, enterprise, or undertaking, or parts of these organizations. It may reference an entire organization, a prime contractor, parent organization, a branch or division, another type of sub-element, a sub-contractor, subsidiary, or other subordinate or connected entity (referred to as ‘‘sub-entities’’ when necessary to distinguish such entities from prime or parent entities). It may also reference a specific location or facility, or the headquarters or official business location of the organization, depending upon the organization’s business structure, the access needs involved, and the responsible Cognizant Security Agency’s (CSA) procedures. The term ‘‘entity’’ as used in the 32 CFR Part 117 Rule refers to the particular entity to which an agency might release, or is releasing, classified information, whether that entity is a parent or subordinate organization.
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.

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, an entity is eligible for access to classified information of a certain level (and all lower levels).
Facility Security Officer (FSO)	A U.S. citizen employee, appointed by a contractor, who will supervise and direct security measures necessary for

F	
	implementing the NISPOM and other Federal requirements for classified information.
FCL System of Record	The DCSA system of record for industrial security oversight accessible by industry, government, and DCSA personnel.
Federal Acquisition Regulation (FAR)	Contains the rules for government acquisition. These rules provide instruction, forms and guidance on government contracting.
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 United States or its territories, and any person who is not a citizen or national of the United States.
Foreign National	Any person who is not a citizen or national of the United States.
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.
Forward Check	A way to verify and validate the records associated with security procedures that begins by reviewing a security record regarding a particular security procedure and then validating the content of the record through interviews and observation.

Back to Top

G	
Government (Security) Review	A government security review is performed by a government representative assigned to your facility by your cognizant security agency, or CSA. Government reviews are conducted at intervals consistent with risk management principles and vary depending on your company's classified involvement. These reviews are usually announced in advance. Government reviews result in the assignment of a security rating.
GSA	General Services Administration. The GSA manages federal property and provides contracting options for government agencies.

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 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 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 Management System (IMS)	A system to protect and control classified information as required by NISPOM. The IMS must be capable of facilitating retrieval and disposition of classified material in a reasonable period of time.
Insider Threat	The likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to contractor or program information to the extent that the information affects the contractor or agency's obligations to protect classified national security information.
Intrusion Detection System (IDS)	A security system that is designed to detect a change in the environment and transmit some type of alarm notification.

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	
Marking	The principal means to inform holders of classified information about specific protection requirements for that information. The marking and designation of classified information are the specific responsibilities of the original and derivative classifiers.

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.
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.

Back to Top

O	
Open Storage Area	An area constructed in accordance with §32 CFR 2001.53 and authorized by the agency head for open storage of classified information.

Back to Top

P	
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.
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.

Back to Top

Q	

Back to Top

R	
Reverse Check	A way to verify and validate the records associated with security procedures that begins with employee interviews or observations and then validates the information gained by reviewing security records.
Risk Management	Risk management is the process of selecting and implementing countermeasures to achieve an acceptable level of risk at an acceptable cost.

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.
Sampling	The technique that involves reviewing a sampling of security records related to a specific security procedure as a means of validating that procedure.
Standard Form (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.
Security Container	A Government Services Administration (GSA) approved security container originally procured through the Federal Supply system. The security containers bear the GSA Approval label on the front face of the container, which identifies them as meeting the testing requirements of the assigned federal specification and having been maintained according to Federal Standard 809.
Security Incident	A security compromise, infraction, or violation.
Security Rating	The National Industrial Security Program (NISP) contractor's security posture is rated as a result of each security review. This rating is a summary description for purposes of the contractor's compliance with the requirements National Industrial Security Program Operating Manual (NISPOM), Industrial Security Letters (ISLs), any other applicable guidance, and the contractor's effectiveness in protecting classified information from unauthorized disclosure or compromise.
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,

S	
	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 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 National Industrial Security Program (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 validates that they not only meet NISPOM requirements, but are 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.
Self- Inspection Handbook	A guide created by DCSA to assist in conducting a self-inspection. It addresses basic NISPOM requirements through a series of questions arranged according to Elements of Inspection.
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.
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.
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. For the purposes of the NISPOM, each subcontractor will be considered as a prime contractor in relation to its subcontractors.

Back to Top

T	
TOP SECRET	The classification level applied to information, the unauthorized disclosure of which reasonable 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

T	
	other classified material from one authorized addressee to another.

Back to Top

U	
Unauthorized Disclosure	A communication, confirmation, acknowledgement, or physical transfer of classified information, including the facilitation of, or actual giving, passing, selling, publishing, or in any way making such information available to an unauthorized recipient.

Back to Top

V

Back to Top

W

Back to Top

X

Back to Top

Y

Back to Top

Z

Back to Top