Glossary

Course: Preparing the DD Form 254, IS128

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

Activity: DoD unit, organization, or installation performing a function or mission.

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 Address Code (AAC): The AAC is 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 DoD for defense agencies.

Administrative Contracting Officer (ACO): The ACO administers the day-to-day activities following the contract award. The ACO may not have official Contracting Officer status but may be a delegate of the Contracting Officer.

Alternative Compensatory Control Measures (ACCM) Information: A Head of a DoD Component with Original Classification Authority (OCA) may employ ACCM when he or she determines that the standard security measures detailed in the DoDM 5200.01-V3 are insufficient to enforce need to know for classified information and SCI or SAP protections are not warranted. The use of an unclassified nickname, obtained in accordance with Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3150.29C (Reference (ae)), together with a list of persons authorized access, and a specific description of information subject to the enhanced ACCM controls, are the three requisite elements of an ACCM.

Classification: Consists of three elements. What needs to be protected, how much protection is required and declassification of National Security information. It is a joint responsibility between the contractor and the U. S. government (GCA).

Classification Levels: Information may be classified at one of the following three levels: TOP SECRET, which is 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; SECRET, which is 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; and CONFIDENTIAL, which is 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.

Classified Contract: Any contract requiring access to classified information by a contractor in the performance of the contract (a contract may be a classified contract even though the contract document is not classified). The requirements prescribed for a "classified contract" also are applicable to all phases of pre-contract activity, including solicitations (bids, quotations, and proposals), pre-contract negotiations, post-contract activity, or other GCA program or project which requires access to classified information by a contractor.

Classification Guide: See Security Classification Guide (SCG)

Classification Guidance: Instruction or source that prescribes classification of specific information

Classified Information: Official information that has been determined, pursuant to Executive Order 12958 or any predecessor order, or pursuant to the Atomic Energy Act of 1954, to require protection against unauthorized disclosure in the interest of national security which has been designated.

Cleared Employees: All contractor employees granted PCLs and all employees being processed for PCLs.

Cognizant Security Agencies (CSAs): Agencies of the Executive Branch that were authorized by Executive Order (EO) 12829 to establish an industrial security program to safeguard classified information under the jurisdiction of these agencies when disclosed or released to U.S. Industry. Those agencies are: The Department of Defense, Office of the Director of National Intelligence, Department of Energy, and the Nuclear Regulatory Commission. EO 13691 established the Department of Homeland Security as a CSA.

Cognizant Security Office (CSO): The organizational entity delegated by the head of a CSA to administer industrial security on behalf of the CSA.

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.

Contract Award: Requires completion of final evaluations and approval of the required clearance documentation and GCA notifies the contractor of the award.

Contract Closeout: During this phase the Contracting Officer must ensure that the work conforms to the requirements in the SOW or PWS. Any deficiencies must be resolved before final payment is made. All classified material must be returned to the GCA or destroyed.

Contracting Officer (CO): The CO has the authority to enter into, administer, and terminate contracts. As well as ensures all contract actions comply with appropriate laws, executive orders, regulations, and other applicable procedures and approvals.

Contracting Officer's Representative (COR): The 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.

Contractor: Any industrial, educational, commercial, or other entity that has been granted an FCL by a CSA.

Contract Manager: The Contract's Manager is 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.

Critical Nuclear Weapons Design Information (CNWDI): A DoD category of TOP SECRET RD or SECRET RD that reveals the theory of operation or design of the components of a thermonuclear or fission bomb, warhead, demolition munition, or test device.

Controlled Unclassified Information (CUI): Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways: Requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify.

Controlled Cryptographic Item (CCI): Secure telecommunications device, or information handling equipment ancillary device, or associated cryptographic component, that is unclassified but controlled. Equipment and components do designed bear the designator “Controlled Cryptographic Item."

Commercial and Government Entity (CAGE) Code: The CAGE Code is a government issued unique identifier used to identify commercial and government entities.

DD Form 254 (DoD Contract Security Classification Specification): Document that 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.

Debriefing: The process of informing a person their need-to-know for access is terminated.

Declassification: The authorized change in the status of information from classified to unclassified information.

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 SCI documents.

Defense Federal Acquisition Regulation Supplement (DFARS): The DFARS implements and supplements the Federal Acquisition Regulation (FAR), and is administered by the Department of Defense (DoD). The DFARS should be read in conjunction with the primary set of rules in the FAR.

Defense Logistics Agency **(DLA):** The DLA is 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 Security Service (DSS): The DSS is an agency of the DoD located in Quantico, Virginia with field offices throughout the United States. The Under Secretary of Defense for Intelligence provides authority, direction and control over DSS. DSS provides the military services, Defense Agencies, 31 federal agencies and approximately 13,500 cleared contractor facilities with security support services.DSS 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. DSS 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.

DSS Center for Development of Security Excellence (CDSE): The CDSE is a nationally accredited, award-winning directorate within the DSS. CDSE provides security education, training, and certification products and services for the DoD and industry.

DSS Industrial Security Field Operations (ISFO): The mission of the DSS ISFO is to provide security oversight of the National Industrial Security Program and minimize vulnerabilities in cleared industry.

Defense Technical Information Center (DTIC): The repository for research and engineering information for the Department of Defense (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 web site.

Department of Defense (DoD): The DoD is an executive branch department of the federal government of the U. S. charged with coordinating and supervising all agencies and functions of the government concerned directly with national security and the United States Armed Forces. The major elements of these forces are the Army, Navy, Marine Corps, and Air Force.

DoD System of Record: The DoD System of Record for this course is referring to the system for Facility Clearances (FCL).

Department of Energy (DOE): The DOE is an executive department of the federal government concerned with the United States' policies regarding energy and safety in handling nuclear material.

Dissemination: The provision of national intelligence to consumers in a form suitable for use.

Downgrade: A determination that classified information requires, in the interest of national security, a lower degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect a lower degree of protection.

Eligibility: A DoD Consolidated Adjudication facility (DoD CAF) has made an adjudicative determination of member's Personnel Security Investigation (PSI) and that member may have access to classified information equal to the level of their adjudicated investigation.

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. (A business or educational organization may consist of one or more facilities as defined herein.) For the purposes of industrial security, the term does not include Government installations.

Facility 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).

Facility Security Officer (FSO): A U.S. citizen employee, appointed by a contractor who will supervise and direct security measures necessary for implementing the NISPOM and other Federal requirements for classified information.

Federal Acquisition Regulation (FAR): Contains the rules for government acquisition. These rules provide instruction, forms and guidance on government contracting.

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.

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.

For Official Use Only (FOUO): FOUO is a security designation used as a handling instruction for Controlled Unclassified Information (CUI) which may be exempt from release under exemptions two through nine of the Freedom of Information Act (FOIA).

Foreign Government Information (FGI): (1) Information provided to the U.S. Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence; (2) information produced by the U.S. pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or (3) information received and treated as "foreign government information" under the terms of Executive Order 12958, as amended, or predecessor order.

Formerly Restricted Data (FRD): Information that has been removed from the RD category after DOE and the DoD have jointly determined that the information: (1) relates primarily to the military utilization of nuclear weapons and (2) can be adequately safeguarded as NSI in the United States.

Freedom of Information Act (FOIA): The Freedom of Information Act (FOIA), found in Title 5 of the United States Code, section 552, is a federal freedom of information law that allows for the full or partial disclosure of previously unreleased information and documents controlled by the United States government.

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

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

Information Security (INFOSEC): The result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information the protection of which is authorized by executive order.

Information Systems (IS): 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 operation.

Invitation For Bid (IFB): A call to contractors to submit a proposal on a project for a specific product or service.

Joint Worldwide Intelligence Communications System (JWICS): A Top Secret/SCI network run by the U. S. Defense Intelligence Agency and used across the DoD, Department of State, Department of Homeland Security and Deportment of Justice to transmit especially sensitive classified information.

NISP Contracts Classification System (NCCS): The NCCS is 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 (NISP): The National Industrial Security Program (NISP) was 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 the National Industrial Security Program Operating Manual (NISPOM), (DoD 5220.22-M).

National Industrial Security Program Operating Manual (NISPOM) – DoD 5200.22M: A manual issued in accordance with the NISP that prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information.

National Intelligence: All intelligence, regardless of the source from which derived and including information gathered within or outside the U.S., that (A) pertains, as determined consistent with any guidance issued by the President, to more than one U.S. Government agency; and (B) that involves: (i) threats to the U.S., its people, property, or interests ; (ii) the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on U .S. national or homeland security.

National Security Information (NSI): Any information that has been determined, pursuant to Executive Order 12958, as amended; or any predecessor order, to require protection against unauthorized disclosure and that is so designated.

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-Accountable SCI: SCI material that does not require document accountability; the DCI has designated SI, TK, G, and HCS as non-accountable SCI.

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.

Office of the Director of National Intelligence (ODNI): Retains authority over access to intelligence sources and methods.

Operations Security (OPSEC): A systematic and proven process intended to deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: (1) identification of critical information; (2) analysis of threats; (3) analysis of vulnerabilities; (4) assessment of risks; and (5) application of appropriate countermeasures.

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.

Prime Contractor: The contractor who receives a prime contract from a GCA and is responsible for disclosing classified information to cleared subcontractors.

Procurement: Procurement is the act of acquiring, buying goods, services or works from an external source, often via a tendering or bid process. It is favorable that the goods, services or works are appropriate and that they are procured at the best possible cost to meet the needs of the acquirer in terms of quality and quantity, time, and location.

Program Manager (PM): Ensures resources are programmed and necessary IP deliverables and associated license rights, tools, equipment, and facilities are acquired to support each of the levels of maintenance that will provide product support and establishes necessary organic depot maintenance capability in compliance with statute and the LCSP.

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

Restricted Data (RD): All data concerning the design, manufacture, or use of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the RD category pursuant to section 142 of reference (c).

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.

SECRET: The classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to national security.

Secret Internet Protocol Router Network (SIPRNET): A system of interconnected computer networks used by the U.S. DoD and the U.S. Department of State to transmit classified information (up to and including information classified SECRET).

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 classified and appropriate declassification instructions. Classification guides for contractors are referenced in the Contract Security Classification Specification (DD Form 254) and provided by the GCA.

Security Inspection: A review of a security program done by the Government Cognizant Security Office. The Security Inspection may be done individually or as a team.

Security Specialist: Also called Activity Security Managers that act as the GCA representatives to the NISP and serve as resident security Subject Matter Experts

(SMEs). They also maintain security cognizance over all activity information, personnel, information systems, physical security and industrial security.

Security Training Education and Professionalization Portal (STEPP): The learning management system used by the Center for Development of Security Excellence (CDSE). STEPP is where the list of courses is maintained and where student information and course transcripts are maintained.

Security Specialist: Also called Activity Security Managers that act as the GCA representatives to the NISP and serve as resident security Subject Matter Experts (SMEs). They also maintain security cognizance over all activity information, personnel, information systems, physical security and industrial security.

Sensitive Compartmented Information (SCI): Compartments that protect national intelligence concerning or derived from intelligence sources, methods, or analytical processes.

Sensitive Compartmented Information Facility (SCIF): An area, room, group of rooms, buildings, or installation certified and accredited as meeting Director of National Intelligence security standards for the processing, storage, and/or discussion of SCI.

Solicitation: This stage is concerned with contract formulation, including the contract form contract clauses, work statement, specifications delivery schedule, and payment terms.

Special Access Program (SAP): Any program that is established to control access, distribution, and to provide protection for particularly sensitive classified information beyond that normally required for TOP SECRET, SECRET, or CONFIDENTIAL information. A Special Access Program can be created or continued only as authorized by a senior agency official delegated such authority pursuant to the NISPOM.

Standard Practice Procedures (SPP): A document(s) prepared by a contractor that implements the applicable requirements of the NISPOM for the contractor's operations and involvement with classified information at the contractor's facility.

Statement of Work (SOW): Designed to describe not only what is to be done but also how it is to be done.

Subcontractor: The contractor who receives a contract, or a portion of a contract from the Prime Contractor or from another subcontractor; and is responsible for disclosing classified information.

Subject Matter Expert (SME): An expert in a particular field who contributes or verifies the accuracy of specific information needed by the project team.

TEMPEST: An unclassified short name referring to the investigation, studies, and control of compromising emanations.

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.

Travel (Official): Travel performed at the direction of the United States Government.

Travel (Unofficial): Travel undertaken by an individual without official, fiscal, or other obligations on behalf of the United States Government.

Unauthorized Disclosure: A communication or physical transfer of classified information to an unauthorized recipient.

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.