Glossary

Course: FSO Role in the NISP

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

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 precontract activity, including solicitations (bids, quotations, and proposals), precontract 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 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.

Classified Information Nondisclosure Agreement: SF 312

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 classified and appropriate declassification instructions. (Classification guides are provided to contractors by the Contract Security Classification Specification)

Classified Visit: A visit during which a visitor will require, or is expected to require, access to classified information.

Cleared Employees: All contractor employees granted PCLs and all employees 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, Central Intelligence Agency, and Nuclear Regulatory Commission.

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.

Compromise: An unauthorized disclosure of information.

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

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

DD Form 254: Contract Security Classification Specification

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.

Defense Security Service (DSS): The Defense Security Service (DSS) is an agency of the Department of Defense (DoD) located in Alexandria, 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, 23 federal agencies and approximately 12,000 cleared contractor facilities with security support services. DSS is the CSO for most DoD classified contracts.

DSS supports national security and the warfighter, secures the nation's technological base, and oversees the protection of US 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 and training, and providing information technology services that support the industrial and personnel security missions of DoD and its partner agencies.

Defense Security Service Academy: A function within the Defense Security Service that provides security education and training to DoD and other U.S. Government personnel and contractors.

Defense Security Service (DSS) Counterintelligence (CI) Office: Office within the Defense Security Service that provides counterintelligence support to DSS through CI reviews, assessments, analysis, and reports.

Defense Security Service Facility Clearance Branch: The Defense Security Service (DSS) Facility Clearance Branch processes contractors for Facility Security Clearance (FCL) based upon procurement need, issues FCLs, and monitors the contractor's continued eligibility in the NISP.

Defense Security Service, Foreign Ownership Control or Influence (FOCI) Office: This office within the Defense Security Service works with the local IS Rep to resolve issues that arise when a cleared facility or a facility being processed for a facility clearance is subject to foreign ownership, control or influence.

Defense Security Service, Office of Designated Approving Authority (ODAA): Office within the Defense Security Service that facilitates the certification and accreditations process for information systems at cleared contractor facilities.

Defense Security Service, Industrial Security Representative (IS Rep): Local representative from the Defense Security Service that provides advice and assistance to establish the security program and to ensure your facility is in compliance with the NISP.

Defense Security Service, Information Systems Security Professional: Local representative from the Defense Security Service, Office of Designated Approving Authority (ODAA) that provides advice and assistance visits to improve the security posture with regard to Information Systems and help facilitate the process of getting your information systems accredited to process classified information.

Department of Defense Consolidated Adjudication Facility (DoD CAF): responsible for issuing a clearance authorization for eligible individuals.

Director of National Intelligence (DNI): retains authority over access to intelligence sources and methods.

Eligibility: A central Adjudication facility (CAF) has made an adjudicative determination of member Personnel Security investigation (PSI) and that member may have access to classified information equal to level of investigation adjudicated.

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 (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).

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.

Field Counterintelligence Specialist (FCIS): Assists FSOs in identifying potential threats to U.S. technology and developing CI awareness and reporting by company employees.

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.

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.

Industrial Security Representative (ISR or IS Rep): The person who represents the Defense Security Service for security matters that are covered by the NISP.

Information Security: 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.

Industrial Security Facilities Database (ISFD): System of record for facility clearance information.

Industrial Security Letters (ISLs): Documents that provide detailed operational guidance and notification of changes to or clarification of existing policies or requirements to the NISPOM.

Information Security Oversight Office (ISOO): Office responsible for implementing and monitoring the NISP and for issuing implementing directives that shall be binding on agencies.

Information System Security Manager (ISSM): An individual appointed by a contractor with oversight responsibility for the development, implementation, and evaluation of the facility's information system security program. The ISSM must be trained to a level commensurate with the complexity of the facility's information systems.

Information System Security Officer (ISSO): ISSOs may be appointed by the ISSM in facilities with multiple accredited information systems. The ISSM will determine the responsibilities to be assigned to the ISSO in accordance with NISPOM Chapter 8.

Information System Security Professional (ISSP): An employee of Defense Security Service assigned to the ODAA or to a DSS field element who provides advice and assistance and participates in certification and inspections of information systems. An ISSP is a subject matter expert on information systems security in the NISP.

Joint Personnel Access System (JAPS): The DoD system of record for contractor eligibility and access for personnel security clearances.

JCAVS: JPAS is comprised of two major subsystems, the Joint Adjudication Management System (JAMS) and the Joint Clearance and Access Verification System (JCAVS). JPAS = JAMS + JCAVS

> JAMS provides Central Adjudication Facilities (CAFs) a single information system to assist in the adjudication process and standardizes core DoD Adjudication processes. JAMS is used by adjudicators to record eligibility determinations and command access decisions, and promotes reciprocity between the DoD CAFs.
>
> JCAVS is one of the two major subsystems of JPAS JCAVS provides security personnel the ability to constantly view eligibility information and update access information in real time. JCAVS also provides users the ability to constantly communicate with other Security Management Offices and CAFs.

Key Management Personnel (KMP): Senior management identified in a facility that require an eligibility determination in order for a facility to be granted a facility clearance.

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.

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): A manual issued in accordance with the National Industrial Security Program that prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified of classified information.

National Security Council (NSC): A governing entity responsible for providing overall policy direction for the National Industrial Security Program.

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.

Personnel Security Management Office for Industry (PSMO-I): Office within the Defense Security Service that processes requests for, and other actions related to personnel security clearances for personnel from facilities participating in the NISP.

Prime Contractor: The contractor who receives a prime contract from a GCA.

SECRET: The classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to national security that the original classification is able to identify or describe.

SF 312: Classified Information Nondisclosure Agreement

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 SERCRET, 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

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.

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 other classified material from one authorized addressee to another.