

## Glossary

### **Course: NISP Reporting Requirements**

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

**Adverse Information:** Any information that adversely reflects on the integrity or character of a cleared employee, that suggest that his or her ability to safeguard classified information may be impaired, that his or her access to classified information clearly may not be in the interest of national security, or that the individual constitutes as insider threat.

**Adjudicative Guidelines:** Guidelines used to determine eligibility for access to classified information or assignment to sensitive duties. There are 13 adjudicative guidelines used to make eligibility determinations.

**Administrative Inquiry:** A broad overview of the investigation that is underway. This is the second step in reporting a security violation.

**Certificate Pertaining to Foreign Interest – SF 328:** A 10-question survey designed to help identify the presence of FOCI in an organization, and provides the basis around which the FOCI analysis process is organized. Completed using e-FCL.

**Central Intelligence Agency (CIA):** The Central Intelligence Agency was created in 1947 with the signing of the National Security Act by President Harry S. Truman. Director Central Intelligence serves as head of the United States intelligence community; act as the principal adviser to the President for intelligence matters related to national security; and serve as head of the CIA.

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

**Classified Information:** 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:** The SF 312 is a non-disclosure agreement required under Executive Order 13292 to be signed by employees of the U.S. Federal Government or one of its contractors before they are granted access to classified information.

**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 Personnel Security Clearances (PCL) 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.

**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.

**Contractor:** Any industrial, educational, commercial, or other entity that has been granted a Facility Clearance (FCL) by a CSA.

**CSA Hotlines:**

Defense Hotline  
The Pentagon  
Washington, DC 20301-1900  
(800) 424-9098

NRC Hotline  
U.S. Nuclear Regulatory Commission  
Office of the Inspector General  
Mail Stop TSD 28  
Washington, DC 20555-0001  
(800) 233-3497

DOE Hotline  
Department of Energy  
Office of the Inspector General

1000 Independence Avenue, SW  
Room SD-031  
Washington, DC 20585  
(202) 586-4073  
(800) 541-1625

DHS Hotline  
Department of Homeland Security  
Office of the Inspector General  
Mail Stop 0305  
245 Murray Lane SW  
Washington, DC 20528  
(800) 323-8603

DNI Hotline  
Director of National Intelligence  
Office of Inspector General  
Washington, DC 20505  
(703) 482-2650

**DD Form 254:** See Department of Defense Contract Security Classification Specification

**DD Form 441:** See Department of Defense Security Agreement

**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.

**Defense Security Service (DSS), Center for Development of Security Excellence (CDSE):** The Center for Development of Security Excellence (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.

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

**Defense Security Service (DSS), Counterintelligence Special Agent (CISA):** Assists FSOs in identifying potential threats to U.S. technology and developing CI awareness and reporting by company employees.

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

**Defense Security Service (DSS), Foreign Ownership Control or Influence (FOCI) Operations Division:** This office within the DSS works with the local Industrial Security Representative (IS Rep) to resolve issues that arise when a cleared facility or a facility being processed for a FCL is subject to FOCI.

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

**Defense Security Service (DSS), Information Systems Security Professional/Security Control Assessor (ISSP/SCA):** Local representative from the DSS, NISP Authorization Office (NAO) that provides advice and assistance, visit to improve the security posture with regard to Information Systems and help facilitate the Assessment and Authorization (A&A) process of Information Systems authorized to process classified information.

**Defense Security Service (DSS), National Industrial Security Program Authorization Office (NAO):** Office within the DSS that facilitates the Assessment and Authorization (A&A) process for classified information systems at cleared contractor facilities.

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

**Department of Defense Contract Security Classification Specification – DD Form 254:** DD Form 254 provides to the cleared contractor, or cleared subcontractor the security requirements and the classification guidance that are necessary to perform on a specific classified contract.

**Department of Defense Security Agreement – DD 441:** A DoD 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.

**Department of Defense System of Record:** This is currently JPAS. In the future JPAS will be replaced by the Defense Information System for Security (DISS).

**Department of Homeland Security (DHS):** In response to the terrorist attacks of September 11, 2001, the Department of Homeland Security (DHS) was created by the Homeland Security Act (HSA) under the administration of President George W. Bush. Their primary objective is to protect U.S. citizens and interests from terrorist attacks.

**eFCL:** DSS's electronic system that all companies must use while in process for a Facility Clearance (FCL) or to report a changed condition.

**Eligibility:** A certified adjudicator at the DoD Central Adjudication Facility (CAF) has made an adjudicative determination that an individual is eligible under national security standards for access to classified information equal to the level of their adjudicated investigation.

**Espionage:** The act or practice of spying or of using spies to obtain secret intelligence. Overt, covert, or clandestine activity, usually used in conjunction with the country against which such an activity takes place (e.g., espionage against the United States (U.S.)).

**Executive Order (EO):** An order issued by the President to create a policy and regulate its administration within the Executive Branch.

**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 security requirements for classified information.

**Federal Bureau of Investigation (FBI):** An intelligence-driven and threat-focused national security organization with both intelligence and law enforcement responsibilities—the principal investigative arm of the U.S. Department of Justice and a full member of the U.S. Intelligence Community.

**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 state in which a contracting agency may find itself in, that may impede its ability to be granted a Facility Security Clearance. The agency will be considered under FOCI if a foreign entity has control, direct or indirect and whether or not exercised, over decisions that affect the management or operation of the organization.

**Government Contracting Activity (GCA):** 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 Facilities Database (ISFD):** The ISFD, maintained by the DSS is a repository of information about DoD cleared contractor facilities. The ISFD has internal users (with full access, such as the DSS IS Reps) and external users (with limited access).

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

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

**Information Systems:** 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 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):** An ISSO 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.

**Individual Culpability:** An individual responsible for a security violation plus evidence of deliberate disregard, gross negligence and a pattern of negligence or carelessness.

**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 impacts the contractor or agency's obligations to protect classified national security information.

**Intrusion Detection System (IDS):** A device or [software application](#) that monitors a [network](#) or systems for malicious activity or policy violations.

**Joint Personnel Access System (JPAS):** The current DoD system of record. In the future JPAS will be replaced by the Defense Information System for Security (DISS).

**Key Management Personnel (KMP):** Key management personnel are Senior Management Officials (SMO) who have the authority to directly or indirectly plan and **control** business operations. KMPs require an eligibility determination before a facility is granted a FCL.

**Limited Access Authorization (LAA):** Security access authorization to CONFIDENTIAL, or SECRET information granted to non-U. S. citizens requiring such limited access in the course of their regular duties.

**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.

**National Industrial Security Program (NISP):** 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 Security Agency (NSA):** Provides information assurance services and information and signals intelligence.

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

**National Security Threat:** An entity capable of aggression or harm to the United States.

**Naturalization:** A process by which U.S. citizenship is granted to a foreign citizen or national after he or she fulfills the requirements established by Congress in the Immigration and Nationality Act (INA).

**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.

**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.

**Preliminary investigation:** The purpose of the preliminary inquiry is to secure the classified information, quickly gather all the facts, and determine if the classified information was subject to loss, compromise, or suspected compromise.

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

**Sabotage:** The willful destruction of government property with the intent to cause injury, destruction, defective production of national defense, or war materials by either an act of commission or omission.

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

**Security 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 for contractors are referenced in the Contract Security Classification Specification (DD Form 254) and provided by the GCA.

**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.

**Security Vulnerability Assessment (SVA):** A review of a contractor security program done by a Defense Security Service Industrial Security Representative. The SVA can be done individually or as a team.

**SF 312:** See Classified Information Nondisclosure Agreement

**SF 328: See Certificate Pertaining to Foreign Interest:** A 10-question survey designed to help identify the presence of FOCI in an organization, and provides the basis around which the FOCI analysis process is organized. Completed using e-FCL.

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

**Subversive Activities:** Subversive activities are willful acts that are intended to be detrimental to the best interests of the government and that do not fall into the categories of treason, sedition, sabotage, or espionage.

**Suspected Compromise:** Occurs whenever identifiable classified information has been made available to unauthorized individual(s) who may have gained access to the information.

**Suspicious Contact:** Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee, all contacts by cleared employees with known or suspected intelligence officers from any country, or any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence services of another country.

**Terrorism:** The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

**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.

**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; information or data transmitted electronically. 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.