

Glossary

Clearances in Industrial Security: Putting It All Together

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

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.

Business Structure: Organization framework legally recognized in a particular jurisdiction for conducting commercial activities, such as sole proprietorship, partnership, and corporation.

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.

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.

Clearance: An administrative authorization for access to National Security Information (NSI) up to a stated classification level (TOP SECRET, SECRET, CONFIDENTIAL).

Cleared Company: A contractor that has been granted FCLs and all contractor facilities being processed for an FCL.

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

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, Office of

the Director of National Intelligence, Department of Energy, Nuclear Regulatory Commission, and Department of Homeland Security.

Commercial and Government Entity (CAGE) Code: A five position code that identifies companies doing or wishing to do business with the federal government. The first and fifth positions in the code must be numeric. The third and fourth positions may be any mixture of alpha/numeric excluding I and O. The code is used to support a variety of mechanized systems throughout the government.

CONFIDENTIAL: The classification level applied to information, the unauthorized disclosure of which could reasonably be expected to cause damage to National Security that the Original Classification Authority (OCA) is able to identify or describe.

Contract Security Classification Specification (DD 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.

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

DD Form 254: *see Contract Security Classification Specification*

DD Form 441: *see Department of Defense (DoD) Security Agreement*

Defense Office of Hearings and Appeals (DOHA): Determine whether an applicant's request for access to classified information is clearly consistent with the national interest to grant or continue security eligibility for the applicant.

Defense Security Service (DSS): An agency of the Department of Defense (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, 30 federal agencies, and approximately 13,500 cleared contractor facilities with security support services. DSS is the CSO for most DoD classified contracts.

DSS supports the National Security and the warfighter, 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 and training, and providing information technology services that support the industrial and personnel security missions of DoD and its partner agencies.

Defense Security Service, Center for Development of Security Excellence (CDSE):

Responsible for providing security education and training to DoD and other U.S. government personnel, DoD contractors, and sponsored representatives of foreign governments.

Defense Security Service, Facility Clearance Branch (FCB): Processes contractors for facility security clearances (FCLs) 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:

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

Defense Security Service, Personnel Security Management Office for Industry (PSMO-I):

Processes requests for and other actions related to personnel security clearances for personnel from facilities participating in the NISP.

Defense Security Service, Special Programs: Manages the security oversight function of DSS's direct and indirect support to the Special Access Program (SAP) community.

Department of Defense (DoD): The largest Cognizant Security Agency (CSA) with the most classified contracts with industry.

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

Department of Defense (DoD) Security Agreement (DD 441): 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.

DOHA: *see Defense Office of Hearings and Appeals*

e-FCL: *see Electronic Facility Clearance System*

e-QIP: *see Electronic Questionnaires for Investigations*

Electronic Facility Clearance System (e-FCL): System that all companies must use while in process for a facility clearance or to report a changed condition.

Electronic Questionnaires for Investigations (e-QIP): An Office of Personnel Management (OPM) software program for the preparation and electronic submission of security forms for a Personnel Security Investigation (PSI) or suitability determination.

Eligibility: The 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 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.

FCL Orientation Handbook: Provides guidance to the Facility Security Officer on the facility security clearance (FCL) process, including business structure and excluded tier entities, the e-FCL process, accounts and systems and preparing for the initial review.

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 Ownership, Control, or Influence (FOCI): Whenever a foreign interest has the power—direct or indirect, whether or not exercised, and whether or not exercisable—to direct or decide matters affecting the management or operations of a company in a manner that may result in unauthorized access to classified information or may adversely affect the performance of classified contracts.

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.

Investigation: The action of investigating something or someone; formal or systematic examination or research.

Investigative Service Provider (ISP): An entity that performs background investigations. The ISP for DoD is the Office of Personnel Management (OPM).

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

JPAS: *see Joint Personnel Adjudication System*

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.

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 the National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M.

National Security: Encompasses both the national defense and the foreign relations of the U.S. Every nation must be able to defend itself, to ensure its own survival and the survival of its way of life. This ability of our nation to defend itself is one aspect of national security. Another way a nation can defend itself is to maintain a good working relationship with other countries, thereby reducing the threat to our nation's survival. For this reason, foreign relations are also part of how we define national security.

Office of Personnel Management (OPM): Provides investigation support for personnel clearances and sponsors the Extranet for Security Professionals online forum.

OPM: *see Office of Personnel Management*

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.

SECRET: The classification level applied to information, the unauthorized disclosure of which could reasonably be expected to cause serious damage to National Security that the Original Classification Authority (OCA) is able to identify or describe.

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.

SAM Database: *see System for Award Management Database*

Secure Web Fingerprint Transmission (SWFT): Web-based system that allows users to submit e-fingerprints and demographic information for personnel security clearance (PCL) applicants.

Security Clearance Package: Package submitted electronically for an initial investigation request. It consists of the Electronic Questionnaires for Investigations Processing (e-QIP), signature forms, and fingerprints via Secure Web Fingerprint Transmission (SWFT).

Sensitive Compartmented Information (SCI): Information that needs extra protection above a Top Secret security clearance level. SCI can come from various sources and has to have special handling, which involves controls to access.

SF 328: Certificate Pertaining to Foreign Interests.

Special Access Program (SAP): Any program that is established to control access and 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.

Sponsorship: The contractor requiring an FCL cannot request a clearance on its own behalf, but instead must be supported (sponsored) by a government entity or by another cleared contractor that is procuring services requiring access to classified information from the uncleared contractor.

Summary Data Sheet: Document containing basic information about a facility such as the facility's website, stock information, and previous names.

SWFT: *see Secure Web Fingerprint Transmission*

System for Award Management (SAM) Database: Secure web portal that consolidates various government acquisition and award capabilities into one system.

TOP SECRET: The classification level applied to information, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to National Security that the Original Classification Authority (OCA) is able to identify or describe.