Glossary

Course: Transmission and Transportation for Industry

Authorized Person: A person who has a need-to-know for classified information in performance of official duties and who has been granted a personnel clearance at the required level.

Cognizant Security Agency (CSA): Agencies of the Executive Branch that have been authorized by reference (a) to establish an industrial security program for the purpose of safeguarding classified information under the jurisdiction of those agencies when disclosed or released to U.S. Industry. These agencies are: The Department of Defense, the Department of Energy, the Central Intelligence Agency, and the 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.

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.

Constant Surveillance Service: A transportation protective service provided by a commercial carrier qualified by SDDC to transport CONFIDENTIAL shipments. The service requires constant surveillance of the shipment at all times by a qualified carrier representative; however, an FCL is not required for the carrier. The carrier providing the service must maintain a signature and tally record for the shipment.

Courier: A cleared employee, designated by the contractor, whose principal duty is to transmit classified material to its destination. The classified material remains in the personal possession of the courier except for authorized overnight storage.

Critical Nuclear Weapon Design Information (CNWDI): CNWDI is 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.

Cryptographic device: A device or piece of equipment which uses cryptographic logic to protect information by converting plain text to cipher text and vice versa.

CSA-approved secure communication: Communication procedures approved by a CSA to securely transmit classified or sensitive information using NSA-approved COMSEC equipment, key material and procedures.

Escort: A cleared person, designated by the contractor, who accompanies a shipment of classified material to its destination. The classified material does not remain in the personal possession of the escort but the conveyance in which the material is transported remains under the constant observation and control of the escort.

Foreign Government Information (FGI): Information that is:

(a) Provided to the US by a foreign government or governments, an international organization of governments or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or
(b) Produced by the US pursuant to, or as a result of, a joint arrangement with a foreign government or governments, an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence.

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

Government-to-Government Channels: Military courier service, diplomatic courier service, military postal channels, or government approved secure electronic communications.

Government-to-Government Transfer: Transfers through government-to-government channels or through other channels that have been agreed in writing by the sending and receiving governments. In the latter case, the procedures must provide for accountability and control from the point of origin to the ultimate destination.

Hand Carriers: A cleared employee, designated by the contractor, who occasionally hand carries classified material to its destination in connection with a classified visit or meeting. The classified material remains in the personal possession of the handcarrier except for authorized overnight storage.

International Program: A lawful and authorized government or commercial effort in which there is a contributing or receiving foreign participant and information or technology is transferred from one country to another.

National Industrial Security Program (NISP): A partnership between the federal government and private industry to safeguard classified information. The NISP was established by Executive Order 12829 to achieve cost savings and protect classified information held by contractors, licensees, and grantees of the United States Government. The Order was signed by President Bush in January of 1993. Redundant, overlapping, or unnecessary requirements impede the technological and economic interests of the U.S Government. Executive Order 12829 calls for a single, integrated, cohesive system for safeguarding classified information held by industry. Consistent with the goal of achieving greater uniformity in security requirements for classified contracts, the four major tenets of the NISP are:

- Achieving uniformity in security procedures.
- Implementing the reciprocity principle in security procedures, particularly with regard to facility and personnel clearances.

- Eliminating duplicative or unnecessary requirements, particularly agency inspections.
- Achieving reductions in security costs.

The NISP affects all executive branch agencies. The major signatories to the program are the Department of Energy, the Nuclear Regulatory Commission, the Department of Defense, and the Central Intelligence Agency.

Need-to-Know: 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.

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.

Prohibited Material: The following material is not authorized for entry into the Defense Courier Service (DCS) system, regardless of classification or other qualifying criteria:

- Contraband, including controlled substances (particularly narcotics and dangerous drugs), as defined in Section 812 of 21 U.S.C.).
- Explosives, ammunition, firearms, and their components.
- Radioactive material, etiological, or other material hazardous to personnel.
- Flammables.
- Liquids.
- Batteries (prohibited from air shipments by the Federal Aviation Administration or international regulations), except as coordinated with the Commander, DCS, in advance.
- Currency, military payment certificates, bonds, securities, precious metals, jewels,
- Postage stamps or other negotiable instruments.

Protective Security Service: A transportation protective service provided by a cleared commercial carrier qualified by the SDDC to transport SECRET shipments.

Reinforced Tape: Reinforced tape consists of a tape base material composed of upper and lower paper layers with a reinforcing thread between the upper and lower paper layers, and a moisture-activated adhesive layer formed on one of surfaces of the tape base material. In thread-reinforced gummed tape, a water-soluble or water-dispersible adhesive is used to laminate the upper and lower paper layers, and a water-soluble thread is used as the reinforcing thread.

Secret: The classification level 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.

Sensitive Compartmented Information (SCI): Sensitive Compartmented Information (SCI) is classified information concerning or derived from intelligence sources, methods, or analytical processes required to be handled within formal access control systems established by the Director of National Intelligence (DNI).

Special Access Program (SAP): Any program that is established to control access, distribution, and to provide protection fro 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 reference (b).

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

System Security Plan (SSP): The SSP is the formal document used by the contractor to identify the protective measures to safeguard information being processed on an Information System in a classified environment.

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 radio, 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.