Glossary

Course: Transmission and Transportation for Department of Defense

Authorized Person: A person who has a favorable determination of eligibility for access to classified information, has signed an approved nondisclosure agreement, and has a need-to-know for the specific classified information in the performance of official duties.

Classified Military Information (CMI): Information originated by or for the Department of Defense or its Agencies or is under their jurisdiction or control and that requires protection in the interests of national security. It is designated TOP SECRET, SECRET, and CONFIDENTIAL, as described in E.O. 13526. Classified military information may be in oral, visual, or material form and has been subdivided further into the eight categories described below:

Category 1 - Organization, Training, and Employment of Military Forces. Information of a general nature pertaining to tactics, techniques, tactical doctrine, and intelligence and counterintelligence doctrine and techniques. Excluded is information necessary for the operation, training, and maintenance on specific equipment covered under Categories 2 and 3, below.

Category 2 - Military Materiel and Munitions. Information on specific items of equipment already in production, or in service, and the information necessary for the operation, maintenance, and training. Items on the U.S. Munitions List fall within this category. This category does not pertain to equipment that is in research and development.

Category 3 - Applied Research and Development Information and Materiel. Information related to fundamental theories, design, and experimental investigation into possible military applications; it includes engineering data, operational requirements, concepts, and military characteristics required to adopt the item for production. Development ceases when the equipment has completed suitability testing and has been adopted for use or production.

Category 4 - Production Information. Information related to designs, specifications, manufacturing techniques, and such related information necessary to manufacture materiel and munitions.

Category 5 - Combined Military Operations, Planning, and Readiness. Information necessary to plan, ensure readiness for, and provide support to the achievement of mutual force development goals or participation in specific combined tactical operations and exercises. It does not include strategic plans and guidance or North American defense information.

Category 6 - U.S. Order of Battle. Information pertaining to U.S. forces in a specific area. In general, disclosures of this information are limited to those countries in which U.S. Forces are stationed or are in adjacent geographical areas.

Category 7 - North American Defense. Information related to plans, operations, programs, and projects, to include data and equipment, directly related to North American defense.

Category 8 - Military Intelligence. Information of a military character pertaining to foreign nations. This category of information does not include national intelligence or sensitive compartmented information under the purview of the Director of Central Intelligence (DCI).

Cognizant Security Agency (CSA): Agencies of the Executive Branch that have been authorized by E.O. 12829 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 Director of National Intelligence, the U.S. Nuclear Regulatory Commission, and the Department of Homeland Security. The Secretary of Defense (SECDEF) has been designated as Executive Agent for the National Industrial Security Program. Heads of the Executive Branches are required to enter into agreements with the SECDEF that establish the terms of the SECDEF's responsibilities on behalf of these agency heads for administration of industrial security on their behalf.

Communications Security (COMSEC): The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications and to ensure the authenticity of such communications. COMSEC includes cryptosecurity, emission security, transmission security, and physical security of COMSEC material and information.

Confidential: "Confidential" shall be 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.

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

Controlled Unclassified Information (CUI): Unclassified information which has been determined to require additional controls and safeguards to prevent inadvertent release to the public. This information is exempt form mandatory release to the public under the Freedom of Information Act.

Courier: A courier is a cleared employee whose principle duty is to transmit classified material to its overnight storage.

Cryptographic System: A cryptographic system is any computer system that involves cryptography. Such systems include for instance, a system for secure electronic mail which might include methods for digital signatures, cryptographic hash functions, key management techniques, etc. Cryptographic systems are made up of cryptographic primitives, and are usually rather complex.

Defense Courier Service (DCS): A joint command and direct reporting unit (DRU) under the Commander in Chief United States Transportation Command (CINCTRANS). The DCS establishes, staffs, operates, and maintains an international network of couriers and courier stations for the expeditious, cost-effective, and secure transmission of qualified classified documents and material.

Escorts: An escort is a cleared employee 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 Disclosure Officer (FDO): Member designated in writing to oversee and control coordination of specific disclosures of classified military information (CMI) and controlled unclassified information (CUI). FDOs are authorized for appointment to lowest command level that is the proponent for created, developed, or derived CMI and CUI and conveying that CMI or CUI through oral or visual means to an authorized representative of a foreign government.

Foreign Government Information (FGI):
(1) Information provided to the United States 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 United States pursuant to or as a result of a joint agreement with a foreign government or governments, or an international organization of governments or any elements 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 a predecessor order.

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.

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.

International Program Security: The total effort that safeguards information and technology identified as requiring control that is generated by, provided to, or transferred in an international program. This includes export/disclosure decision and security arrangements.

JWICS: Joint Worldwide Intelligence Communications System is the Sensitive Compartmented Information (SCI) portion of the Defense Information Systems Network (DISN). It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing.

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

Need-to-Know: A criterion used in security procedures that requires the custodians of classified information to establish, prior to disclosure, that the intended recipient must have access to the information to perform or assist in a lawful and authorized governmental function.

OPSEC: Operations Security (OPSEC) is a systematic and proved process by which the U.S. Government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive Government activities.

Program Security Guide (PSG): Security policy for a specific program under the direction of the Program Security Officer (PSO)

Program Security Officer (PSO): The government official who administers the security policies for a Special Access Program (SAP)

Prohibited Electronic Device (PED): Any electronic device prohibited from being introduced or its presence allowed in a classified space

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.

Protected Distribution System (PDS): A wire line or fiber optics distribution system with adequate electrical, electromagnetic, and physical safeguards to permit its use for the transmission of unencrypted classified information.

Protective Security Service (PSS): A transportation protective service provided by a cleared commercial carrier qualified by the Surface Deployment and Distribution Command (SDDC) to transport SECRET shipments. The carrier must provide continuous attendance and surveillance of the shipment by qualified carrier representatives and maintain a signature and tally record. In the case of air movement, however, observation of the shipment is not required during the period it is stored in the carrier's aircraft in the connection with flight, provided the shipment is loaded into a compartment that is not accessible to an unauthorized person aboard. Conversely, if the shipment is loaded into a compartment of the aircraft that is accessible to an unauthorized person aboard, the shipment must remain under the constant surveillance of a cleared escort or qualified carrier representative.

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.

SAP: A Special Access Program (SAP) is any DoD program or activity as authorized in E.O. 13526 employing enhanced security measures (e.g., safeguarding, access requirements, etc.) exceeding those normally required for collateral information at the same level of classification.

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).

Secret: "Secret" shall be 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.

SIPRNET: Secret Internet Protocol Router Network (SIPRNET) is a worldwide Secret-level packet switch network that uses high-speed internet protocol routers and high-capacity Defense Information Systems Network (DISN) circuitry.

Status of Forces Agreement (SOFA): A document that defines the legal status of U.S. personnel and property in the territory of another nation. The purpose of such an agreement is to set forth rights and responsibilities between the United States and the host government on such matters as criminal and civil jurisdiction, the wearing of the uniform, the carrying of arms, tax and customs relief, entry and exit of personnel and property, and resolving damage claims.

Top Secret: "Top Secret" shall be 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.

Transmission and Transportation: The transmission and transportation of information from one place to another may occur by radio, microwave, laser, or other non-connective method, as well as by cable, wire or other connective medium. Transmission and transportation also includes the physical transfer of material from a sender to a recipient.