A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A	
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.

Back to Top

B	

Back to Top

C	
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 interest of national security. It is designated TOP SECRET, SECRET, and CONFIDENTIAL, as described in E.O. 13526.
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 (DOD), the Department of Energy (DOE), the Director of National Intelligence (DNI), the U.S. Nuclear Regulatory Commission (NRC), and the Department of Homeland Security (DHS).
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	Information or material of which unauthorized disclosure could reasonably be expected to cause damage to national security that the Original Classification Authority (OCA) 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.

C	
Controlled Unclassified Information (CUI)	Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.
Courier	Cleared employee whose principle duty is to transmit classified material to its overnight storage.
Cryptographic System	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.

Back to Top

D	
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.

Back to Top

E	
Escorts	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.

Back to Top

F	
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).

F	
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.

Back to Top

G	
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.

Back to Top

H	

Back to Top

I	
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.

Back to Top

J	
Joint Worldwide Intelligence Community Systems (JWICS)	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.

Back to Top

K	

Back to Top

L	

Back to Top

M	

Back to Top

N	
National Industrial Security Program (NISP)	A partnership between the federal government and 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.
National Security	Information relating to the national defense or foreign relations of the United States.
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.

Back to Top

O	
Operations Security (OPSEC)	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.
Original Classification Authority (OCA)	An individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to originally classify information.

Back to Top

P	
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	Material not authorized for entry into the Defense Courier Service (DCS) system, regardless of classification or other qualifying criteria.
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.

Back to Top

Q

Back to Top

R	
Reinforced Tape	Tape which 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.

Back to Top

S	
Special Access Program (SAP)	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.

S	
Sensitive Compartmented Information (SCI)	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	Information or material of which, unauthorized disclosure could reasonably be expected to cause serious damage to national security that the Original Classification Authority (OCA) is able to identify or describe.
Secret Internet Protocol Router Network (SIPRNET)	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.

Back to Top

T	
Top Secret	Information or material of which, unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to national security that the Original Classification Authority (OCA) 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.

Back to Top

U

Back to Top

V

Back to Top

W

Back to Top

X

Back to Top

Y

Back to Top

Z

Back to Top