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

Term	Definition
Access	The ability and opportunity to gain knowledge of classified information. Access equals eligibility plus need-to-know plus a signed SF 312.
Authorized Source	Derivative classifiers must only refer to authorized sources when determining classification markings which include security classification guides, or a properly marked source document.
Automatic Declassification	Declassification of information that is more than 25 years old and is not otherwise prevented from being declassified by an approved exemption. Such information shall be declassified on the 31st of December, 25 years from the date of original classification.

Back to Top

B

Term	Definition
Banner Marking	Indicate the highest level of classification of the overall document, as determined by the highest level of any one portion within the document. They are placed on the top and bottom of every page of the document.

Back to Top

C

Term	Definition
Center of Development of Security Excellence (CDSE)	Provides security education and training to Department of Defense (DOD) and other U.S. Government personnel, DOD contractors, and sponsored representatives of foreign governments.
Classification	The act or process by which information is determined to require protection against unauthorized disclosure and is marked to indicate its classified status.
Classification Authority Block (CAB)	Identifies who the document was classified by—the reason the information was classified (for an original document), or from which source the information is derived (if a derivative document). It indicates the classification level to downgrade to at a certain point in time, if applicable, and the declassification date and is placed on the face of each classified document near the bottom.
Classified National Security Information	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 and is marked to indicate its classified status when in documentary form.

Term	Definition
Classified Information Nondisclosure Agreement	SF 312, a contractual agreement between the U.S. Government and a cleared employee that must be executed as a condition of access to classified information.
Classifier	An individual who makes a classification determination and applies a security classification to information or material.
Compilation	Items of information that are individually unclassified or classified at a lower level, may be classified, or classified at a higher level, only if the compiled information reveals an additional association or relationship.
Compromise	An unauthorized disclosure of classified information.
Confidential (C)	Information or material of which unauthorized disclosure could reasonably be expected to cause damage to national security that the Original Classification Authority is able to identify or describe.
Contained in	Applies when derivative classifiers incorporate classified information, word for word, from an authorized source into a new document, and no additional interpretation or analysis is needed to determine the classification of that information.
Controlled Unclassified Information (CUI)	Information the U. S. Government creates or possesses, or that an entity creates or possesses for or on behalf of the U.S. Government, that a law, regulation, or U.S. Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information.
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.
Custodian	An individual who has possession of, or is otherwise charged with, the responsibility for safeguarding classified information.
Cybersecurity	Measures that protect and defend information and information systems.

Back to Top

D

Term	Definition
Declassification	An authorized change in status of information from classified to unclassified.
Defense Counterintelligence and Security Agency (DCSA)	The federal government's largest security agency in the federal government dedicated to protecting America's trusted workforce and trusted workspaces.
Defense Courier Division (DCD)	A DOD entity responsible for the secure transport of classified documents and materials.

Term	Definition
Defense Office of Prepublication and Security Review (DOPSR)	Responsible for managing the DOD security review program and reviewing written materials for public and controlled release.
Department of Defense (DOD)	Provides the military forces needed to deter war and protect national security. Under the President, the Secretary of Defense directs and exercise authority and control over the separately organized Departments of the Air Force, the Army, and the Navy; over the Joint Chiefs of Staff; over the combatant commands; and over defense agencies and field activities.
Department of Defense Directive (DODD)	A formal, written instruction issued by the Secretary of Defense or the Deputy Secretary of Defense that establishes policy, assigns responsibilities, and prescribes procedures within the Department of Defense.
Department of Defense Instruction (DODI)	A formal document that implements policy established in a Department of Defense Directive (DODD) like a "how-to" manual that puts the policy into practice.
Department of Defense Manual (DODM)	Provides detailed procedures and guidance to implement policies and procedures outlined in both Department of Defense Directives (DODDs) and Department of Defense Instructions (DODIs).
Derivative Classification	Incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information.
Derivative Classifiers	All cleared DOD and authorized contractor personnel who generate or create new material from sources which are already classified.
Destruction	Destroying classified information so that it can’t be recognized or reconstructed.
Dissemination	The sharing or transmitting of classified information to others who have authorized access to that information.
Document	Any physical medium in or on which information is recorded or stored, to include written or printed matter, audiovisual materials, and electromagnetic storage material.
Downgrading	A determination by an OCA or declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.
Duration	A determination made regarding how long information is to be protected (i.e., when the information will lose its sensitivity and no longer merit or qualify for classification).

Back to Top

E

Term	Definition
Eligibility	DCSA Adjudication and Vetting Services (AVS) formerly known as the Department of Defense Consolidated Adjudications Facility (DOD CAF) has made an adjudicative determination of a member's Personnel Security Investigation (PSI) and that member may have access to classified information equal to the level of their adjudicated investigation.
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. Is also an individual that is required to accompany an uncleared individual or visitor to a contractor facility.
Evaluated Products List (EPL)	A list of destruction products that have been tested and meet performance requirements.
Exceptions	Permanent exclusions or deviations put in place when classified information cannot be safeguarded to the standards or requirements specified in DODM 5200.01,Volume 1, Enclosure 3.
Executive Order (EO)	An order issued by the President to create a policy and regulate its administration within the Executive Branch.
Executive Order (E.O.) 13526	Establishes the legal authority for certain officials within the Executive Branch of the Federal government to designate classified national security information (CSNI).

Back to Top

G

Term	Definition
General Services Administration (GSA)	Federal agency which establishes and publishes uniform standards, specification, and supply schedules for units and key-operated and combination padlocks suitable for the storage and protection of classified information.
Government Information (Official)	A step in the original classification process; for information to be identified as official, it must be owned by, produced by or for, or under the control of the U.S. Government.

Back to Top

I

Term	Definition
Impact	A step in the original classification process that assesses the probable operational, technological, and resources of classification.
Information	Knowledge that can be communicated, and documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the U.S. Government.
Information Security	The system of policies, procedures, and requirements established in accordance with EO 13526 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security. The term also applies to policies, procedures and requirements established to protect controlled unclassified information, which may be withheld from release to the public in accordance with statue, regulation, or policy.
Information Security Oversight Office (ISOO)	Oversees programs for classified national security information and controlled unclassified information in both Government and Industry, and reports on their status annually to the President.
Information Security Program (ISP)	Implements policy, assign responsibilities, and provide procedures for the designation, marking, protection, and dissemination of controlled unclassified information (CUI) and classified information, including information categorized as collateral, sensitive compartmented information (SCI), and Special Access Program (SAP).
Information System (IS)	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.

Back to Top

L

Term	Definition
Loss	The inability to physically locate or account for classified information.

Back to Top

M

Term	Definition
Mandatory Declassification Review	A way for members of the public to request the review of specific classified information.
Markings	Serve to alert holders to the presence of classified information and technical information with restriction on its dissemination; identify, as specifically as possible, the exact information that needs protection; indicate the level of classification assigned to the information; provide guidance on downgrading and declassification; give information on the source or sources and reason or reasons for classification or other restrictions; and warn holders of special access, control, or safeguarding requirements.

Back to Top

N

Term	Definition
National Security	Information relating to the national defense or foreign relations of the United States.
National Security Administration (NSA)	Agency of the Federal Government that maintains listings of evaluated destruction products that have been tested and meet performance requirements and provides information assurance services and information and signals intelligence.

Back to Top

O

Term	Definition
Original Classification	An initial determination that information requires, in the interests of national security, protection against unauthorized disclosure
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.
"Owned by"	Information that belongs to the U.S. Government.

Back to Top

P

Term	Definition
Portion Marking	Indicates the highest level of classification in every portion of the document and must be placed at the beginning of the respective portion.
"Produced by"	Government-developed information
"Produced for"	When the government enters into an agreement through purchase, lease, contract, or receipt of the information as a gift.

Term	Definition
Properly Marked Source Document	An authorized source of classification guidance used by a derivative classifier, from which information is extracted, paraphrased, restated, and/or generated in a new form for inclusion in another document.

Back to Top

R

Term	Definition
"Revealed by"	Applies when classified information has been paraphrased or restated and not taken word for word from an authorized source document, but the classification is deduced from interpretation or analysis.

Back to Top

S

Term	Definition
Safeguarding	Refers to using prescribed measures and controls to protect classified information.
Scheduled Declassification	A set date or event, determined by the Original Classification Authority (OCA), which will occur within 25 years from the date of original classification.
Secret (S)	Information or material of which unauthorized disclosure could reasonably be expected to cause serious damage to national security that the Original Classification Authority is able to identify or describe.
Security Classification Guidance	Guidance that details the classification of a system(s), plan(s), program(s), mission(s), or project(s) issued by an Original Classification Authority to document and disseminate classification decisions under their jurisdiction.
Security Classification Guide (SCG)	A comprehensive document issued by an OCA that provides mandatory instructions on how to classify information, derivatively classify information, and declassify information**.** This classification guidance specifically identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each element.
Security Incidents	When someone fails to use proper security requirements for protecting classified information. There are two types of security incidents, security violations and security infractions.
Security Infraction	A failure to comply with security requirements which cannot reasonably be expected to, and does not result in the loss, suspected compromise or compromise of classified information.

Security Manager	Manages and implements the DOD activity's Information Security Program (ISP) on behalf of the activity head, to whom he or she shall have direct access.
Security Violation	Occurs when there is a knowing, willful, or negligent action that could reasonably be expected to result in the loss, suspected compromise, or compromise of classified information.
Sensitive Compartmented Information (SCI)	Information that needs extra protection above a Top Secret security classification level. SCI can come from various sources and has to have special handling, which involves controls to access.
SF 312	Classified Information Nondisclosure Agreement
SF 700	Security Container Information, used to maintain a record for each container and to record the combination.
SF 701	Activity Security Checklist, used to record checks of work areas at the end of each working day.
SF 702	Security Container Check Sheet, used to record the securing of vaults, rooms, and containers used for storing classified material.
SF 703	Cover sheet for TOP SECRET material
SF 704	Cover sheet for SECRET material
SF 705	Cover sheet for CONFIDENTIAL material
Spillage	Is a type of security violation that occurs when classified data is introduced on an information system not approved for that level of information.
Systematic Declassification	Review of classified information that has been exempted from automatic declassification.

Back to Top

T

Term	Definition
Top Secret (TS)	Information or material of which unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to national security that the Original Classification Authority is able to identify or describe.
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. 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.

Back to Top

U

Term	Definition
Unauthorized Disclosure (UD)	A communication or physical transfer of classified information to an unauthorized recipient.
Under Secretary of Defense for Intelligence and Security (USD(I&S))	Provides implementation guidance for the Information Security Program within the DOD.

Back to Top

W

Term	Definition
Waivers	Temporary exclusions or deviations put in place when classified information cannot be safeguarded to the standards or requirements specified in DODM 5200.01, Volume 1.

Back to Top