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	
Access	The ability and opportunity to obtain knowledge of classified information. Access equals eligibility plus need-to-know plus a signed SF-312.
Activity Security Checklist	SF-701 – Completed when it has been verified that all areas have been secured.
Adjudication	The evaluation of pertinent data in a background investigation, as well as any other available information that is relevant and reliable, to determine whether a covered individual is suitable for Government employment.
Adversary	An individual, group, country, or organization that can cause harm to people, resources, or missions.
Adverse Information	Any information that adversely reflects on the integrity or character of a cleared employee, which suggests that his or her ability to safeguard classified information may be impaired or that his or her access to classified information clearly may not be in the interest of National Security.
Authorized Person	A person (recipient) who has a favorable determination of eligibility for access to classified information, has signed a SF 312, and has a need to know for the specific classified information in the performance of official duties.

Back to Top

B	
Banner Lines	Indicates 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	
Chemical Decomposition	To separate into constituent parts or elements or into simpler compounds using a chemical element.
Classification Authority Block (CAB)	Indicates who the document was classified by, where it was derived from, downgrade instructions, and when it should be declassified. The CAB is placed on the face of each classified document near the bottom.
Classification by Compilation	Occurs when unclassified elements of information are combined to reveal classified information, or

C	
	when classified elements combine to reveal information at a higher classification level than the individual elements.
Classified Information	Information that has been determined pursuant to EO 13526, or any successor order, EO 12958, or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011) to require protection against unauthorized disclosure and that is marked to indicate its classified status when in documentary form.
Classified Information Non-disclosure 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. Required to access classified information.
Cleared Contractor	A person or facility operating under the National Industrial Security Program (NISP) that has had an administrative determination that they are eligible, from a security point of view, for access to classified information of a certain level (and all lower levels).
Cleared Employee	A person who has been granted access to classified information, other than the President and Vice President; employed by, or detailed or assigned to, a department or agency, including members of the Armed Forces; or any other category of person who acts for or on behalf of a department or agency as determined by the appropriate department or agency head.
Common Access Card (CAC)	Standard form of identification for DOD employees.
Compromise	An unauthorized disclosure of classified information. Occurs when classified information is disclosed to a person who does not have an appropriate security eligibility, authorized access, or need-to-know.
Confidential	Information or material of which unauthorized disclosure could reasonably be expected to cause damage to national security that the OCA is able to identify or describe.
Continuous Evaluation	The process to review the background of an individual who has been determined to be eligible for access to classified information or to hold a sensitive position at any time during the period of eligibility. CE leverages a set of automated record checks and business rules to assist in the on-going assessment of an individual's continued eligibility (EO 13467, as amended). The CE process begins once an initial adjudicative determination is made and continues

C	
	until the individual is no longer eligible for access to classified information or to hold a sensitive position.
Controlled Unclassified Information (CUI)	Unclassified information associated with a law, regulation, or government-wide policy and identified as needing safeguarding.
Controlled Unclassified Information Executive Agent (CUI EA)	The CUI EA is the National Archives and Records Administration (NARA), which implements the executive branch-wide CUI Program and overseas Federal agency actions to comply with E.O. 13556. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO).
Countermeasure	The employment of devices or techniques that impair the operational effectiveness of enemy activity. Countermeasures may include anything that effectively negates an adversary's ability to exploit vulnerabilities.
Courier	A cleared employee, 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.
Courier Authorization Card	DD Form 2501 – Issued when there is a continuing need to escort or hand-carry classified information.
Courier Briefing	A briefing provided to the courier prior to the courier assignment. It must inform the courier of the requirements and responsibilities of escorting or hand-carrying.
Courier Letters	Also known as the authorization letter. This letter provides authorization for travel aboard commercial passenger aircraft. It must be on the agency letterhead and in its original form, not a reproduced copy.
Critical-Sensitive	A position sensitivity designation indicating the potential for exceptionally grave impact on the integrity or efficiency of the service or on the national security.

Back to Top

D	
Damage to the National Security	Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

D	
Declassification	The authorized change in the status of information from classified information to unclassified information.
Defense Office of Prepublication and Security Review (DOPSR)	Responsible for reviewing written materials both for public and controlled release to ensure information that is publically released does not contain classified, controlled unclassified information, or other information that in aggregate may lead to a compromise of national security.
Degaussing	To remove or neutralize the magnetic field of a material.
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DODM	Department of Defense Manual
Departments and Agencies	Refers to any "Executive agency," as defined in 5 U.S.C. 105; any "Military department," as defined in 5 U.S.C. 102; any "independent establishment," as defined in 5 U.S.C. 104; and any other entity within the executive branch that comes into the possession of classified information.
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. Includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.
Director of National Intelligence (DNI)	The Security Executive Agent (SecEA) responsible for ensuring reciprocal recognition of national security eligibility among the agencies.
Dissemination Controls	Controls agencies may use these controls to limit or specify who should or should not receive the information.
Downgrade	A determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

Back to Top

E	
Eligibility	A DOD Consolidated Adjudication facility (DOD CAF) has made an adjudicative determination of a member's Personnel Security Investigation (PSI) and that member may have access to classified

E	
	information equal to the level of their adjudicated investigation.
Espionage	Espionage is a national security crime; specifically, it violates Title 18 USC, §§ 792-798 and Article 106a, Uniform Code of Military Justice (UCMJ). Espionage convictions require the transmittal of national defense information with the intent to aid a foreign power or harm the U.S. However, even gathering, collecting, or losing national defense information can be prosecuted under Title 18.
Executive Order 13467	Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information. Expanded on Intelligence Reform and Terrorism Prevention Act (IRTPA) requirements to further align and guide reform efforts within the U.S. Government.
Executive Order 13526	Classified National Security Information. Establishes the legal authority for certain officials within the Executive Branch of the Federal Government to designate classified national security information.

Back to Top

F	
Facility 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). FCL is also referred to as an entity eligibility determination.
Federal Investigative Standards (FIS)	A five-tiered investigative model developed in accordance with Executive Order 13467. The FIS sets standard requirements used to conduct background investigations that determine eligibility to access classified information or hold a national security sensitive positon.
Foreign Contacts	Contact with individuals of any foreign nationality, either within or outside the scope of your official duties.
Foreign National	Any person who is not a citizen or national of the United States.

Back to Top

G	
General Services Administration (GSA)	Federal agency that establishes and publishes uniform standards, specification, and supply schedules for units and key-operated and

G	
	combination padlocks suitable for the storage and protection of classified information.

Back to Top

H	
Hand-carry	To transport classified material to its destination. The classified material remains in the personal possession of the hand carrier except for authorized overnight storage.

Back to Top

I	
Incorporating	The act of blending or combining already classified information into a newly formed document.
Information Security Oversight Office (ISOO)	Develops and issues implementing guidance and is responsible for implementing and monitoring the National Industrial Security Program.
Information Security Program	Defined as the system of policies, procedures, and requirements established to protect classified and controlled unclassified information, or CUI that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security.
Information Systems	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.
Intrusion Detection System (IDS)	Used to deter, detect, document, deny, or delay intrusion by detecting a change in the environment. These systems can be exterior or interior and include sensors, control units, transmission lines, and monitor units.

Back to Top

J

Back to Top

K

Back to Top

L	
Loss	Classified information that is or was outside the custodian's control and the classified information cannot be located or its disposition cannot be determined. A spillage always results in a loss.

Back to Top

M	
Markings	Alert holders to the presence of classified information and technical information with restrictions on its dissemination, provides guidance on information sharing and downgrading and declassification as well as warn holders of special access, control, or safeguarding requirements.
Mutilation	The act or instance of damaging or altering something radically.

Back to Top

N	
National Archives and Records Administration (NARA)	Preserves U.S. Government records, manages the Presidential Libraries system, and publishes laws, regulations, Presidential, and other public documents.
National Industrial Security Program Operating Manual (NISPOM)	A manual issued in accordance with the National Industrial Security Program (NISP) that prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information.
National Interest	The interest of a nation as a whole held to be an independent entity separate from the interests of subordinate areas or groups and also of other nations or supranational groups.
National Security	A collective term encompassing both national defense and foreign relations of the United States.
National Security Agency (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.
National Security Eligibility	Favorable determination that affords an individual eligibility for access to classified information or assignment to a national security sensitive position.
National Security Eligibility Program	Ensures members of the Armed Forces, DOD civilian employees, DOD contractor personnel, and other affiliated persons are granted access to classified information and/or assignment to a national security sensitive position consistent with the interests of national security.

N	
National Security Information	Information that has been determined, pursuant to E.O. 13526, to require protection against unauthorized disclosure and is so marked when in documentary form.
Need-to-Know	A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.
Negligent Discharge of Classified Information (NDCI)	Violation that occurs when data is placed on an information technology system with insufficient controls to protect the data at the required classification.
Non-Critical Sensitive	Position requires eligibility for access to Secret or Confidential level information and has the potential for significant or serious damage to National Security. (Tier 3)
Non-Sensitive	Position requires no clearance or other sensitive National Security duties. (Tier 1)

Back to Top

O	
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.
Office of Personnel Management (OPM)	Manages the civil service of the federal government and coordinates recruiting of new government employees.
Open Storage	A room or area constructed and operated for the purpose of safeguarding national security information that, because of its size or nature or operations necessity, cannot be adequately protected by the normal safeguards or stored during nonworking hours in approved security containers.
Operating System	Software that controls the operation of a computer and directs the processing of programs (as by assigning storage space in memory and controlling input and output functions).
Operations Security (OPSEC)	Process of identifying critical information and analyzing friendly actions attendant to military operations and other activities.
Original Classification	An initial determination that information requires (in the interests of national security) protection against unauthorized disclosure.

O	
Overwriting	To replace information in (a computer file) with new information.

Back to Top

P	
Paraphrasing	A restatement of a text, passage, or work, giving the meaning in another form.
Periodic Reinvestigation	A national security investigation conducted to update a previously completed investigation on persons holding a national security position or performing national security duties to determine whether that individual continues to meet national security requirements.
Personally Identifiable Information (PII)	Information used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, biometric records, home phone numbers, other demographic, personnel, medical, and financial information. PII includes any information that is linked or linkable to a specified individual, alone, or when combined with other personal or identifying information.
Personnel Security Investigation (PSI)	An inquiry into the activities of an individual, designed to develop pertinent information pertaining to trustworthiness and suitability for a position of trust as related to loyalty, character, emotional stability, and reliability.
Personnel Security Program (PSP)	Program aimed to protect national security by ensuring only loyal, trustworthy, and reliable individuals may access classified information and/or be assigned to national security sensitive positions.
Physical Security Program	The program concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.
Portion Markings	Classification markings placed before paragraphs, subjects, titles, graphics, tables, charts, bullet statements, sub-paragraphs, classified signature blocks, and other portions within slide presentations and the like.
Pre-publication Process	The process by which written material is reviewed in order for all the information to be disclosed to the public.
Privacy Act of 1974	The Privacy Act of 1974 (5 USC §552a) establishes a code of fair information practices that governs the

P	
	collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.
Protection	Includes all controls an agency applies or must apply when handling classified or controlled unclassified information.
Public Media	A medium of communications designed to reach the public. Public media includes print media (e.g., newspapers, magazines, books), broadcast media (e.g., radio, television), and Internet media (e.g., websites, blogs, tweets).
Pulverizing	Crushing, beating, or grinding (something) into powder or dust.

Back to Top

Q	

Back to Top

R	
Restating	To state again or in another way.

Back to Top

S	
Sabotage	An act or acts with the intent to injure or interfere with or obstruct the national defense of a country by willfully injuring, destroying, or attempting to destroy any national defense or war materiel, premises, or utilities, including human or natural resources, under reference.
Safeguarding	Measures and controls that are prescribed to protect classified information.
Secret	Information or material of which unauthorized disclosure could reasonably be expected to cause serious damage to national security that the OCA is able to identify or describe.
Security Container Check Sheet	SF-702 – Annotated when security containers have been verified to be opened or closed.
Security Container Information	SF-700 – Used to record the combinations to security containers, secure rooms, and controlled area doors and to identify personnel to be contacted if a container or facility are found open and unattended.
Security Forces	Made up of DOD, military, and contract personnel and trained dogs.

S	
Security Incident	When someone fails to use proper security requirements for protecting classified information. There are four types, security violations, security infraction, spillage, and unauthorized disclosure.
Security Infraction	Any knowing, willful, or negligent action contrary to Executive Order 13526 or its implementing directives that does not constitute a security violation.
Security Manager	Maintain security cognizance over all activity information, personnel, information systems, physical security, and industrial security. They also act as the GCA representatives to the NISP and serve as resident security subject matter experts (SMEs).
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.
Self-Reporting	To provide information on one's self.
Sensitive Compartmented Information (SCI)	Classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established by the Director of National Intelligence.
SF 312	Classified Information Non-disclosure Agreement
SF 700	Security Container Information
SF 701	Activity Security Checklist
SF 702	Security Container Check Sheet
SF 703	Cover sheet for Top Secret Information
SF 704	Cover sheet for Secret Information
SF 705	Cover sheet for Confidential Information
SF 706	Top Secret media label
SF 707	Secret media label
SF 708	Confidential media label
SF 710	Unclassified media label
Special Sensitive	Position requires eligibility for access to Sensitive Compartmented Information (SCI)/Top Secret (TS) or Special Access Program (SAP) level information and has the potential for inestimable damage to National Security. (Tier 5)
Suitability	Refers to a person's identifiable character traits and/or conduct that may have an impact on the integrity or efficiency of the service.

Back to Top

T	
Terrorism	The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.
Threats	Adversaries who have the intent, capability, and opportunity to cause loss or damage.
Tier 3	Background investigation for non-critical sensitive, Confidential, and Secret Information
Tier 5	Background investigation for critical sensitive, special sensitive Top Secret, and Sensitive Compartmented Information (SCI)
Top Secret (TS)	Information or material of which unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to national security that the OCA is able to identify or describe.

Back to Top

U	
Unauthorized Disclosure	A communication or physical transfer of classified information to an unauthorized recipient.
Unauthorized Persons	A person not authorized to have access to specific classified information in accordance with policy requirements.

Back to Top

V	
Violation	Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information.

Back to Top

W	
Wet Pulping	Using a wet machine usually containing 50 to 65 percent of water to deteriorate material.
Whole person concept	Looks at all available and reliable information about an individual's past and present prior to reaching an adjudicative determination.
Working papers	Working papers can be rough drafts, notes, or anything that is not a finished document.

Back to Top

X	

Back to Top

Y

Back to Top

Z

Back to Top