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-701is the Activity Security Checklist that is completed for end of day security checks. This checklist is completed at the close of each duty and/or business day to ensure that any area where classified information is used or stored is secure.
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.
Antiterrorism	Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include rapid containment by local military and civilian forces.
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	
Barriers and Fencing	Used to establish boundaries and deter individuals from gaining access to DOD assets.

Back to Top

C	
Continuous Vetting (CV)	The step of the vetting process when trusted individuals undergo continuous review to ensure the government and public's confidence that an individual will continue to protect people, property, information, and mission. CV will replace the five- and 10-year periodic reviews with ongoing and automated determinations of a person's security risk. CV assesses risk in near real-time to provide insight into trusted insider behavior.
Controlled Unclassified Information (CUI)	CUI is information that requires safeguarding or dissemination controls consistent with applicable laws, regulations, or government-wide policies, but is not classified information under Executive Order 13526 or the Atomic Energy Act.

Back to Top

D	
Damage (to 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.
Defense Counterintelligence and Security Agency, Consolidated Adjudications Services (DCSA, CAS)	DCSA has two fundamental missions: personnel security and industrial security. Supporting these two core missions are counterintelligence and insider threat and security training.
Defense Office of Prepublication and Security Review (DOPSR)	Responsible for reviewing written materials both for public and controlled release to ensure information that is publicly released does not contain classified, controlled unclassified information, or other information that in aggregate may lead to a compromise of national security.
Department of Defense (DOD)	Provides the military forces needed to deter war and ensure our nation's security.
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.
Defense Federal Acquisition Regulation Supplement (DFARS)	The DFARS is an amendment to a set of rules that DOD uses to oversee the purchasing of goods and services, including technology. DFARS regulations help guarantee the integrity of CUI, or sensitive

D	
	information belonging to the government that third parties such as contractors, suppliers, or other partners trade associations may hold or use.
Dissemination Controls	Controls agencies may use to limit or specify who should or should not receive the information.
DODI	Department of Defense Instruction
DODM	Department of Defense Manual
Driving Under the Influence (DUI)	The offense of operating a motor vehicle while intoxicated by drugs or especially alcohol.
Driving While Intoxicated (DWI)	Driving while affected by alcohol or drugs especially to the point where physical and mental control is markedly diminished.

Back to Top

E	
Eligibility	DCSA Consolidated Adjudication Services (DCSA CAS) 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.
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.

Back to Top

F	
Federal Personnel Vetting Investigative Standards (FIS)	A three-tiered investigative model developed in accordance with Executive Order 13467. The FIS sets standard requirements used to conduct

F	
	background investigations that determine eligibility to access classified information or hold a national security sensitive position. With the implementation of Trusted Workforce 2.0, the original five-tier personnel vetting investigative standards were modified to better meet suitability, fitness, national security, and credentialing decisions further enabling greater workforce mobility.
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 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.
Initial Vetting	Conducts the vetting needed to establish trust with an individual not previously vetted; includes a preliminary determination process to onboard individuals based on the early results of high-yield records check.
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.
Information Security Oversight Office (ISOO)	Develops, coordinates and issues implementing directives and instructions regarding Executive Orders 13526 and 13556. Reviews and approves the

I	
	implementing regulations issued by the executive branch agencies.

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)	NARA is the nation's record keeper. Their mission is providing equitable public access to federal government records in their custody and control.
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.
Need-to-Know	A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in

N	
	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.

Back to Top

O	
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.
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.
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	
Paraphrasing	The derivative classification concept that refers to rewording classified information in a new derivative document.
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.
Prepublication Review Process	The process of reviewing written material before it can be disclosed to the public.

P	
Protection	Includes all controls an agency applies or must apply when handling classified or controlled unclassified information.
Pulverizing	Crushing, beating, or grinding (something) into powder or dust.

Back to Top

Q	

Back to Top

R	
Restating	The derivative classification concept that refers to stating classified information in another way in a new derivative document.

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 of could reasonably be expected to cause serious damage to national security that the Original Classification Authority (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 Department of Defense (DOD), military, and contract personnel and trained dogs.
Security Incident	When someone fails to use proper security requirements for protecting classified information. Security incidents typically involve a security procedure that was not in place or was not followed properly, such as unsecured classified documents, improper receipt of foreign government information (FGI) per 32 CFR § 117.8 (c)(13), or spillage involving classified information on an unclassified

S	
	network. There are two types of security incidents, security infractions and security violations.
Security Infraction	A security infraction is a security incident that does not result in the loss, compromise, or suspected compromise of classified information.
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 oneself.
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 (DNI).
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

Back to Top

T	
Threats	Adversaries who have the intent, capability, and opportunity to cause loss or damage.
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 (OCA) is able to identify or describe.
Trusted Workforce (TW) 2.0	The effort to improve the personnel security clearance process and the issue of security clearance timeliness, while implementing a risk-based process that looks more strategically at which types of behaviors and positions constitute a security risk – and which do not. The revamped vetting will focus on mission needs, outlining five specific vetting scenarios.

Back to Top

U	
Unauthorized Disclosure (UD)	Any communication or physical transfer of classified information or CUI to an unauthorized recipient.
Unauthorized Persons	A person not authorized to have access to specific classified information or controlled unclassified 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.

Back to Top

X

Back to Top

Y

Back to Top

Z

Back to Top