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	
Approval to Operate (ATO)	Approval granted by an Authorizing Official (AO) for an information system to process classified information.
Assessment	Testing and evaluating the security controls applied to an information system to ensure the controls are correctly implemented, operating as intended, and meet the security requirements for the system.
Assurance	Measure of confidence that the security features, practices, procedures and architecture of an information technology (IT) system accurately mediates and enforces the security policy.
Authorization	Official decision by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations
Authorizing Official	Senior official or executive with the authority to formally assume responsibility for operating an IS at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and national security.

Back to Top

B

Back to Top

C	
Classified Contract	Any contract that requires or will require access to classified information by a contractor or his or her employees in the performance of the contract. (A contract may be a classified contract even though the contract document is not classified.) The requirements prescribed for a “classified contract” also are applicable to all phases of pre-contract activity, including solicitations (bids, quotations, and proposals), pre-contract negotiations, post-contract activity, or other Information Owner (IO) program or project which requires access to classified information by a contractor.
Classified Information	Official information that has been determined, pursuant to Executive Order 12958 or any predecessor order, to require protection against unauthorized disclosure in the interest of national security and which has been so designated. The term includes National Security Information (NSI), Restricted Data (RD), and Formerly Restricted Data (FRD).

Cognizant Security Agency (CSA)	Agencies that have been authorized by Executive Order (EO) 12829 to establish an industrial security program to safeguard classified information under the jurisdiction of those agencies when disclosed or released to U.S. Industry.
Cleared Contractor	Any industrial, educational, commercial, or other entity that has been granted a Facility (Security) Clearance (FCL) by a Cognizant Security Authority (CSA).

Back to Top

D	
Denial of Authorization to Operate (DATO)	Formal decision made by the Authorizing Official that an IS cannot operate.

Back to Top

E

Back to Top

F	
Facility	A plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, that, when related by function and location, form an operating entity. (A business or educational organization may consist of one or more facilities as defined herein.) For purposes of industrial security, the term does not include Government installations.
Facility Security Officer (FSO)	Supervise and direct security measures necessary for implementing applicable requirements of the NISPOM and related Federal requirements for classified information.
Formal Access Approval	Formal Access Approval is the documented approval by a data owner to allow access to a particular category of information. It can be linked to any caveated information such as compartmented, NATO, REL TO, Critical Nuclear Weapon Design Information, COMSEC or Crypto variable information, FRD, etc.

Back to Top

G

Back to Top

H

Back to Top

I	
Impact Level	The impact level (low, moderate, or high) for the information processed by an information system is defined based on the confidentiality, integrity, and availability of the information. Security requirements vary depending on the impact level of the information.

Information Owner (IO)	An organizational official (must be a U.S. citizen and government employee) with statutory, management, or operational authority for specific information who has the responsibility for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal of classified information.
Industrial Security	That portion of information security which is concerned with the protection of classified information in the custody of U.S. industry.
Information System	Any telecommunication or computer-related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of voice or data, and includes software, firmware and hardware.
Information System Security Manager (ISSM)	The cleared contractor employee responsible for the implementation of system security, and operational compliance with the documented security measures and controls, at the cleared contractor facility.
Information System Security Officer (ISSO)	The ISSO is assigned by the ISSM when the facility has multiple authorized systems, is in a multiple facility organization in which the ISSM has oversight responsibility for multiple facilities, or when the technical complexity of the facility's system security program warrants the appointment.
Interim Approval to Connect (IATC)	Temporary approval granted by a WAN AO allowing the connection of a node to WAN.

Back to Top

J

Back to Top

K

Back to Top

L

Back to Top

M

Multiple Facility Organization Network	A legal entity (single proprietorship, partnership, association, trust, or corporation) that is composed of two or more facilities.

Back to Top

N

Network Security Plan	Documents the security posture of interconnection between two or more separately accredited information systems

Back to Top

O	

Back to Top

P	
Plan of Action and Milestones (POA&M)	Facilitates an agreement between the contractor and DCSA identifying items from the baseline configuration requirements cannot be met and the reasons. The POA&M documents deficiencies that can be corrected and defines a timeline for resolving the issues.

Back to Top

Q	

Back to Top

R	
Reassessment	An action taken by DCSA when security relevant changes are made to an approved Security Plan.
Reauthorization	An action taken by DCSA when security relevant changes are made to an approved system. An action taken by DCSA when the Authorization Termination Date (ATD) has been reached.
Risk	A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting impact.
Risk Assessment	Process of analyzing threats to, and vulnerabilities of, a system, and the potential impact that the loss of information or capabilities of a system would have on national security. The resulting analysis is used as a basis for identifying appropriate and effective measures.
Risk Management	Process concerned with the identification, measurement, control, and minimization of security risks in information technology (IT) systems to a level commensurate with the value of the assets protected.
Risk Management Framework (RMF)	Establishes a common set of guidelines for the assessment and authorization of ISs and provide a holistic and strategic process for the risk management of information systems.
Risk Mitigation	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

Back to Top

S	
Security Controls	Safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.
Security Control Assessor (SCA)	Is an individual(s) appointed by the Authorizing Official to act on their behalf in the oversight of contractor IS processing classified information.
Security Relevant Change	A security-relevant change to a system is any change

	affecting the availability, integrity, authentication, confidentiality, or non-repudiation of a system or its environment.
Security Plan (SP)	Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
Security Content Automation Protocol (SCAP) Compliance Checker	Automated compliance scanning application that utilizes Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) benchmarks and Operating System (OS) specific baselines to analyze and report on the security configuration of the system. The application can be run locally on the host system to be scanned, or scans can be conducted across a network.

Back to Top

T

Threat	The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

Back to Top

U

User	Person or process authorized to access an information technology (IT) system.

Back to Top

V

Verification	The process of determining compliance of the evolving information technology (IT) system specification, design, or code with the security requirements and approach agreed on by the users, acquisition authority, and the Authorizing Official (AO).
Vulnerability	A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

Back to Top

W

Back to Top

X

Back to Top

Y

Back to Top

Z

Back to Top