

[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

<b>Adjudication</b>	Evaluation of personnel security investigations and other relevant information to determine if it is clearly consistent with the interests of national security for persons to be granted (or retain) eligibility for access to classified information and continue to hold positions requiring trustworthiness decision.
<b>Adverse Information</b>	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, that his or her access to classified information clearly may not be in the interest of national security, or that the individual constitutes an insider threat.
<b>Assessment and Authorization (A&amp;A)</b>	The standard DoD approach for identifying information systems security requirements, providing security solutions and managing the security of DoD Information Systems.
<b>Assistant Facility Security Officer (AFSO)</b>	Assists the Facility Security Officer with their security duties.

[Back to Top](#)

## B

[Back to Top](#)

## C

<b>Center for Development of Security Excellence (CDSE)</b>	A nationally accredited, award-winning directorate within the DSS. CDSE provides security, training and certification products and services for the DoD and Industry.
<b>Classified Information</b>	Official information that has been determined, pursuant to DoD 5220.22-M reference (b) 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 NSI, RD and FRD.
<b>Cognizant Security Agency (CSA)</b>	Agencies of the Executive Branch that have been authorized by DoD 5220.22-M reference (a) to establish an industrial security program to safeguard classified information under the jurisdiction of those agencies when disclosed or related to U.S. Industry. These agencies are: The Department of Defense, DOE, CIA, and NRC.
<b>Commercial and Government Entity (CAGE) Code</b>	A five position code that identifies companies doing, or wishing to do, business with the Federal government. The first and fifth positions in the code must be numeric. The third and fourth positions may be any mixture of alpha/numeric excluding I and O. The code is used to support a variety of mechanized systems throughout the government.

C

<b>Common Access Card (CAC)</b>	The standard identification for active duty uniformed Service personnel, Selected Reserve, DoD civilian employees and eligible contractor personnel. It is also the principal card used to enable physical access to buildings and controlled spaces, and it provides access to DoD computer network and systems.
<b>Contract Security Classification Specification (DD Form 254)</b>	DD Form 254 provides to the cleared contractor or cleared subcontractor the security requirements and the classification guidance that are necessary to perform on a specific classified contract.
<b>Contractor</b>	Any industrial, educational, commercial, or other entity that has been granted an FCL by a CSA.
<b>Contractor Performance Assessment Reporting System (CPARS)</b>	CPARS is a web-enabled application that collects and manages the library of automated Contractor Performance Assessment Reports (CPARs). A CPAR assesses a contractor's performance and provides a record, both positive and negative, on a given contractor during a specific period of time. Each assessment is based on objective facts and supported by program and contract management data, such as cost performance reports, customer comments, quality reviews, technical interchange meetings, financial solvency assessments, construction/production management reviews, contractor operations reviews, functional performance evaluations, and earned contract incentives.
<b>Counterintelligence (CI)</b>	Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs.

[Back to Top](#)

D

<b>Defense Central Index of Investigations (DCII)</b>	An automated Department of Defense repository that identifies investigations conducted by Department of Defense investigative agencies and personnel security determinations made by Department of Defense adjudicative authorities.
<b>Defense Information System for Security (DISS)</b>	DISS will replace the Joint Personnel Adjudication System (JPAS). DISS consists of two main components, the Case Adjudication Tracking System (CATS) and the DISS Portal which will replace the Joint Clearance and Access Verification System (JCAVS).
<b>Defense Manpower Data Center (DMDC)</b>	Serves under the Office of the Secretary of Defense (OUSD) to collate personnel, manpower, training, financial, and other data for the Department of Defense. DMDC operates and maintains the DCII system.

D

<b>Defense Security Service (DSS)</b>	The DSS is an agency of the DoD located in Quantico, Virginia. The Under Secretary of Defense for Intelligence provides authority, direction and control over DSS. DSS supports national security and the service members, secures the nation's technological base, and oversees the protection of U.S. and foreign classified information in the hands of industry. DSS accomplishes this mission by clearing industrial facilities, accrediting information systems, facilitating the personnel security clearance process, delivering security education, training, and certification and providing information technology services that support the industrial and personnel security missions of DoD and its partner agencies.
<b>Department of Defense (DoD)</b>	The DoD is an executive branch department of the federal government of the U. S. charged with coordinating and supervising all agencies and functions of the government concerned directly with national security and the United States Armed Forces. The major elements of these forces are the Army, Navy, Marine Corps, and Air Force.

[Back to Top](#)

E

<b>Electronic Application (eAPP)</b>	Developed by the Defense Information Systems Agency, eAPP is designed to help federal security clearance applicants submit applications for background investigations. Electronic Application will replace Electronic Questionnaires for Investigations Processing (eQIP).
<b>Electronic Questionnaires for Investigations Processing (eQIP)</b>	A secure, automated, web-based system that facilitates the processing of standard investigative forms used in background investigations for federal security, suitability, fitness, and credentialing purposes.
<b>Electronic Subcontracting Reporting System (eSRS)</b>	Eliminates the need for paper submissions and processing of the SF 294's, Individual Subcontracting Reports, and SF 295's, Summary Subcontracting Reports, and replaces the paper with an easy-to-use electronic process to collect the data.
<b>Enterprise Mission Assurance Support Service (eMASS)</b>	A government-owned web-based application with a broad range of services for comprehensive fully integrated cybersecurity management.
<b>Excluded Parties List System (EPLS)</b>	Electronic directory of individuals and organizations that are not permitted to receive federal contracts or assistance from the United States government.
<b>Executive Order (EO)</b>	An order issued by the President to create a policy and regulate its administration within the Executive Branch.
<b>External Certification Authority (ECA)</b>	A Department of Defense (DoD) program to support the issuance of DoD-approved certificates to industry partners and other external entities and organizations. The program is designed to provide the mechanism for these entities to

E

securely communicate with the DoD and authenticate to DoD information systems.

[Back to Top](#)

F

<b>Facility</b>	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 in the NISPOM.) For purposes of industrial security, the term does not include Government installations.
<b>Facility (Security) Clearance (FCL)</b>	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).
<b>Facility Clearance Branch (FCB)</b>	The Defense Security Service Facility Clearance Branch processes contractors for Facility Security Clearances based upon procurement need, issues FCLs, and monitors the contractor's continued eligibility in the National Industrial Security Program.
<b>Facility Verification Request (FVR)</b>	Function to verify a contractor's facility clearance, locations, and address.
<b>Federal Bureau of Investigation (FBI)</b>	The Federal Bureau of Investigation is an intelligence-driven and threat-focused national security organization with both intelligence and law enforcement responsibilities – the principal investigative arm of the U. S. Department of Justice and a full member of the U. S. Intelligence Community.
<b>Federal Security Officer (FSO)</b>	A U.S. citizen employee, appointed by a contractor who will supervise and direct security measures necessary for implementing the NISPOM and other Federal requirements for classified information.
<b>Foreign Ownership, Control, or Influence (FOCI)</b>	A company is considered to be operating under Foreign Ownership, Control or Influence whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts.

[Back to Top](#)

G

<b>Government Contracting Activity (GCA)</b>	An element of an agency designated by the agency head and delegated broad authority regarding acquisition functions.
--	--

[Back to Top](#)

H

<b>Human Intelligence (HUMINT)</b>	Category of intelligence derived from information collected and/or provided by human sources.
------------------------------------	---

[Back to Top](#)

I

<b>Industrial Security Field Operations (ISFO)</b>	Provides oversight and conducts security vulnerability assessments for approximately 13,500 cleared contractor facilities. They maintain industrial security field offices all over the country.
<b>Industrial Security Representative (IS Rep)</b>	Local representative from the Defense Security Service that provides advice and assistance on security matters and with establishing your security program to ensure your facility is in compliance with the NISP.
<b>Information System Security Manager (ISSM)</b>	An individual appointed by a contractor with oversight responsibility for the development, implementation, and evaluation of the facility's information system security program. The ISSM must be trained to a level commensurate with the complexity of the facility's information systems.
<b>Information System Security Professional/Security Control Assessor (ISSP/SCA)</b>	An employee of Defense Security Service assigned to the ODAA or to a DSS field element who provides advice and assistance and participates in certification and inspections of information systems. An ISSP is a subject matter expert on information systems security in the NISP.
<b>Interconnection Security Agreement (ISA)</b>	An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/A) between the organizations.
<b>Investigation Service Provider (ISP)</b>	Reviews the security clearance package for completeness to open the investigation.

[Back to Top](#)

J

<b>Joint Adjudication Management System (JAMS)</b>	Provides Central Adjudication Facilities (CAFs) a single information system to assist in the adjudication process and standardizes core DoD Adjudication processes. It is used by adjudicators to record eligibility determinations and command access decisions, and to promote reciprocity between the DoD and CAFs.
<b>Joint Clearance Access and Verification System (JCAVS)</b>	<p>JPAS is comprised of two major subsystems, the Joint Adjudication Management System (JAMS) and the Joint Clearance and Access Verification System (JCAVS).</p> <p>JPAS = JAMS + JCAVS.</p> <p>JAMS provides Central Adjudication Facilities (CAFs) a single information system to assist in the adjudication process and standardizes core DoD Adjudication</p>

J

processes. JAMS is used by adjudicators to record eligibility determinations and command access decisions and promotes reciprocity between the DoD CAFs. JCAVS is one of the two major subsystems of JPAS. JCAVS provides security personnel the ability to constantly view eligibility information and update access information in real time. JCAVS also provides users the ability to constantly communicate with other Security Management Offices and CAFs.

**Joint Personnel Security System (JPAS)**

Joint Personnel Security System is the master repository and centralized processing tool that provides the capability to perform personnel security management of DoD civilian employees, military personnel, and DoD contractors.

[Back to Top](#)

K

**Key Management Personnel (KMP)**

Key management personnel are Senior Management Officials (SMO) who have the authority to directly or indirectly plan and control business operations. KMPs require an eligibility determination before a facility is granted an FCL.

[Back to Top](#)

L

[Back to Top](#)

M

[Back to Top](#)

N

**National Industrial Security Program (NISP)**

National Industrial Security Program; serves as a single integrated, cohesive industrial security program to protect classified information and preserve our Nation's economic and technological interests.

**National Industrial Security Program Central Access Information Security System (NCAISS)**

Secure web portal that allows single sign-on access to various DSS applications used in the NISP.

**National Industrial Security Program Contract Classification System**

NISP Contract Classification System; NCCS is an automated web-based system and centralized repository that allows for the collection and querying of DD Form 254, DoD Contract Security Classification Specification, data.

**National Industrial Security Program Office (NAO)**

Office within the DSS that facilitates the Assessment and Authorization (A&A) process for classified information systems at cleared contractor facilities.

**National Industrial Security System (NISS)**

National Industrial Security System; NISS is the system of record for facility clearance information.

[Back to Top](#)

## O

<b>Office of the Chief Information Officer (OCIO)</b>	A job title commonly given to the most senior executive in an enterprise who works with information technology and computer systems, in order to support enterprise goals.
<b>Office of the Under Secretary of Defense (OUSD) for Acquisition &amp; Sustainment OSUD(A&amp;S)</b>	Focused on forming an acquisition system that moves at the speed of relevance, and to do that, has been shaped into an organization that provides a defense-wide adaptive acquisition framework from need identification to disposal.

[Back to Top](#)

## P

<b>Personally Identifiable Information (PII)</b>	PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.
<b>Personnel (Security) Clearance (PCL)</b>	An administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted.

[Back to Top](#)

## Q

<b>Questionnaire for National Security Positions (SF-86)</b>	Standard Form 86 developed by the Office of Personnel Management for background investigations and reinvestigations. Completed by the applicant, the Questionnaire for National Security Positions provides details on various aspects of the individual's personal and professional background.
<b>Questionnaire for Non-Sensitive Positions (SF-85)</b>	Standard Form 85 developed by the Office of Personnel Management for background investigations and reinvestigations. Completed by the applicant, the Questionnaire for Non-Sensitive Positions.
<b>Questionnaire for Public Trust Positions (SF-85P)</b>	Standard Form 85P developed by the Office of Personnel Management for background investigations and reinvestigations. Completed by the applicant, the Questionnaire for Public Trust Positions.

[Back to Top](#)

## R

--	--

[Back to Top](#)

## S

<b>Secure Web Fingerprint Transmission (SWFT)</b>	Secure Web Fingerprint Transmission; SWFT is a web-based system that enables cleared defense industry users to submit e-fingerprints for applicants who require investigation for a personnel security clearance.
<b>Security, Training, Education, and Professionalization Portal (STEPP)</b>	The learning management system used by the Center for Development of Security Excellence (CDSE). STEPP is

## S

where the list of courses is maintained and where student information and course transcripts are maintained.

### **System for Award Management (SAM)**

Secure web portal that consolidates various government acquisition and award capabilities into one system.

### **System Security Authorization Agreement (SSAA)**

Formal document that fully describes the planned security tasks required to meet system or network security requirements. The package must contain all information necessary to allow the Designated Approving Authority to make an official management determination for authorization for a system, or site to operate in a particular security mode of operation; with a prescribed set of safeguards, against a defined threat with stated vulnerabilities and countermeasures; in a given operational environment; under a stated operational concept; with stated interconnections to external systems; and at an acceptable level of risk.

### **System Security Plan (SSP)**

see System Security Authorization Agreement

[Back to Top](#)

## T

[Back to Top](#)

## U

[Back to Top](#)

## V

### **Vetting Risk Operations Center (VROC)**

Office within the DSS that processes requests for, and other actions related to, personnel security clearances for personnel from facilities participating in the NISP.

[Back to Top](#)

## W

[Back to Top](#)

## X

[Back to Top](#)

## Y

[Back to Top](#)

## Z

[Back to Top](#)