NISP TERMS AND ACRONYMS, IN PLAIN LANGUAGE

115 terms an FSO meets in the National Industrial Security Program, 67 of them acronyms, each with what it means, where the rule says so and where this site covers it. Type a few letters to filter the list, or jump to a letter.

Go to the terms

How this glossary is kept

IN SHORT

Every entry links to its authority, most often a paragraph of 32 CFR Part 117 (the NISPOM) or a Security Executive Agent Directive, and to the page here that covers the topic. Each term has a fixed address, such as /glossary/#foci, so any page or email can point straight at it.

A

Access

The ability and opportunity to gain knowledge of classified information. A contractor may give an employee access only at or below the FCL level, and only with a valid need-to-know, a favorable eligibility determination at that level and a signed nondisclosure agreement.

Authority: 32 CFR §117.3; 32 CFR §117.10(a)(1)(iii) **On this site:** Access and lifecycle **See also:** Eligibility, Need-to-know, NDA

ACCM

Stands for: *Alternative compensatory control measures*

Extra security measures an agency applies to specific classified intelligence or operations when the normal protections are judged insufficient. A contractor takes part only when the DD Form 254 (or equivalent) identifies the access and the associated security plan.

Authority: 32 CFR §117.3; 32 CFR §117.23(c) **On this site:** DD Form 254 item 10

Adjudicative guidelines

The thirteen guidelines, A through M, that an adjudicator weighs under SEAD 4 when deciding whether someone is eligible for access to classified information: for example Guideline B, Foreign Influence, and Guideline F, Financial Considerations. Each guideline lists the conditions that raise a concern and those that mitigate it.

Authority: SEAD 4, Appendix A **On this site:** DOHA decisions by guideline · Adjudication Atlas **See also:** SEAD 4

Adverse information

Information that reflects badly on a cleared employee's integrity or character, suggests their ability to protect classified information may be impaired, suggests their access may not be in the interest of national security, or indicates an insider threat. Contractors must report it to the CSA; rumor and innuendo are not reported.

Authority: 32 CFR §117.3; 32 CFR §117.8(c)(1) **On this site:** Adverse information reports **See also:** SEAD 3

B

Board resolution

The lightest FOCI measure: when a foreign interest owns shares but cannot elect or otherwise claim a seat on the board, the governing board resolves to identify the foreign holder, describe its shares, acknowledge the company's NISP obligations and keep the foreign interest away from classified information and the company's security program.

Authority: 32 CFR §117.11(d)(2)(i) **On this site:** FOCI mitigation compared **See also:** FOCI, SCA, SSA

C

CAGE code

Stands for: *Commercial and Government Entity code*

The five-character identifier the Defense Logistics Agency assigns to a business location. A company needs one before it can be sponsored for an FCL, and FAR 4.402 requires the CAGE code of each contractor named on a DD Form 254.

Authority: 32 CFR §117.3; FAR 4.402(d); DLA CAGE program **On this site:** FCL sponsorship · FCL readiness check · DD Form 254 item 6

CCIPP

Stands for: *Classified critical infrastructure protection program*

The Department of Homeland Security program for sharing classified information with critical-infrastructure partners under E.O. 13691. A CCIPP eligibility determination is not an FCL and does not qualify for FCL reciprocity.

Authority: 32 CFR §117.3; 32 CFR §117.22

CDC

Stands for: *Cleared defense contractor*

A contractor cleared under the NISP that holds classified contracts with the Department of Defense. CDCs carry the additional cyber-incident reporting duty in §117.8(f), which rests on DFARS 252.204-7012.

Authority: 32 CFR §117.3; 32 CFR §117.8(f) **On this site:** Cyber incident reports **See also:** DFARS 252.204-7012

CDSE

Stands for: *Center for Development of Security Excellence*

DCSA's security training organization: it runs the FSO orientation and program management courses the rule expects, the FSO and insider threat toolkits, and STEPP, the portal where cleared industry takes its training.

Authority: 32 CFR §117.12(d); CDSE FSO Toolkit **On this site:** Keeping the FCL **See also:** STEPP

CFIUS

Stands for: *Committee on Foreign Investment in the United States*

The interagency committee that reviews foreign investment in U.S. businesses for national security risk under 31 CFR Part 800. The SF 328 borrows its definition of a foreign person; a CFIUS review and DCSA's FOCI determination are separate processes that can run on the same transaction.

Authority: 32 CFR §117.11(j); 31 CFR 800.224 **On this site:** SF 328 guide · FOCI mitigation compared

Changed condition

An event that affects a company's FCL and must be reported to the CSA: a change of ownership or control, operating name or address, KMP, any action to end the business or enter bankruptcy, or a material change in FOCI (reported with an updated SF 328). Changes in storage capability and the inability to safeguard are reported under their own paragraphs.

Authority: 32 CFR §117.8(c)(7); 32 CFR §117.8(c)(8) **On this site:** Entity and facility changes · Where changed-condition packages go **See also:** NISS, Entity Vetting (EV)

Classification levels

Confidential, Secret and Top Secret: the three levels of classified national security information, applied according to whether unauthorized disclosure could reasonably be expected to cause damage, serious damage or exceptionally grave damage to national security. An FCL or PCL at one level covers that level and everything below it.

Authority: 32 CFR §117.3; 32 CFR §117.9(a)(7) **On this site:** DD Form 254 item 1

Classified contract

Any contract, license, agreement or grant that requires a contractor and its employees to have access to classified information to perform. The contract document itself need not be classified, and the requirements reach every phase from solicitation to close-out.

Authority: 32 CFR §117.3 **On this site:** DD Form 254 guide **See also:** DD Form 254

Cleared employee

An employee of a contractor, licensee, grantee or subcontractor whom a CSA has found eligible for access to classified information, or who is being processed for that determination. The reporting rules in §117.8 and SEAD 3 apply to this whole group, not only to people with current access.

Authority: 32 CFR §117.3 **On this site:** Cleared industry reporting

Closed area

An area that meets the rule's safeguarding requirements for classified material which, because of its size, nature or operational need, cannot be protected by the normal safeguards or stored in approved containers outside working hours. Approval of a closed area, like any storage approval, is separate from the FCL.

Authority: 32 CFR §117.3; 32 CFR §117.15 **On this site:** FCL readiness check: storage **See also:** Possessing and non-possessing facility

CMMC

Stands for: *Cybersecurity Maturity Model Certification*

DoD's program for verifying, before award, that a contractor handling Federal contract information or CUI meets the cybersecurity requirements in FAR 52.204-21 and NIST SP 800-171, at Levels 1 to 3. It concerns unclassified systems and sits outside the NISPOM, though many cleared contractors must satisfy both.

Authority: 32 CFR Part 170 **On this site:** CMMC and cybersecurity news **See also:** CUI, DFARS 252.204-7012

CNWDI

Stands for: *Critical nuclear weapon design information*

A DoD category of Top Secret or Secret Restricted Data that reveals the theory of operation or design of the components of a nuclear weapon. Access is held to the absolute minimum, employees are briefed by the FSO before access, and it appears as its own box on the DD Form 254.

Authority: 32 CFR §117.3; 32 CFR §117.20 **On this site:** DD Form 254 item 10 **See also:** Restricted Data (RD) and Formerly Restricted Data (FRD)

Compromise
An unauthorized disclosure of classified information. Any loss, compromise or suspected compromise of U.S. or foreign classified information must be reported to the CSA, with a preliminary inquiry and a final report to follow.

Authority: 32 CFR §117.3; 32 CFR §117.8(d) **On this site:** Loss or compromise reports **See also:** Security violation

COMSEC
Stands for: *Communications security*

The measures that deny unauthorized people information from U.S. Government telecommunications about national security and that authenticate those communications. Classified COMSEC is proscribed information, is handled through a COMSEC account under a central office of record, and needs its own briefing before access.

Authority: 32 CFR §117.3; 32 CFR §117.21 **On this site:** DD Form 254 item 10 · National interest determinations **See also:** COR, Proscribed information

Consultant
In the NISPOM, an individual under contract and paid directly to give a contractor professional or technical help in a role that needs access to classified information; for security purposes the consultant is treated as the hiring contractor's employee. A security consultant who advises an FSO without classified access is a different matter, and cannot replace the FSO the company must appoint.

Authority: 32 CFR §117.3; 32 CFR §117.10(m) **On this site:** Hiring an FSO consultant

Continuous evaluation (CE)
The SEAD 6 process of automated records checks on people already found eligible, meant to supplement rather than replace scheduled reinvestigations. In current practice the term has given way to continuous vetting under Trusted Workforce 2.0.

Authority: 32 CFR §117.3; SEAD 6, Continuous Evaluation **On this site:** Continuous vetting updates **See also:** CV, SEAD 6

Contractor
In the NISPOM, any industrial, educational, commercial or other entity that a CSA has granted an entity eligibility determination, including licensees, grantees and certificate holders. The word refers to the company, never to its employees.

Authority: 32 CFR §117.3 **See also:** FCL, Cleared employee

COR
Stands for: *Central office of record*

In the NISPOM, the office that establishes and keeps account of a contractor's COMSEC material; it sets up the COMSEC account once the contracting officer says one is needed and approves the account managers. In general contracting, COR means a contracting officer's representative, so check which is meant.

Authority: 32 CFR §117.3; 32 CFR §117.21(d) **See also:** COMSEC

CSA
Stands for: *Cognizant security agency*

An agency with NISP implementation and security responsibility for its own components and for the contractors and other agencies under its cognizance. There are five: the Department of Defense, the Department of Energy, the Nuclear Regulatory Commission, the Office of the Director of National Intelligence and the Department of Homeland Security.

Authority: 32 CFR §117.3; 32 CFR §117.6 **On this site:** Who decides eligibility and access **See also:** CSO, DCSA

CSO
Stands for: *Cognizant security office*

The organizational unit to which the head of a CSA delegates the day-to-day administration of industrial security. DCSA is the DoD CSO, which is why most cleared contractors deal with DCSA rather than with DoD directly.

Authority: 32 CFR §117.3; 32 CFR §117.6(b) **On this site:** Receiving DCSA oversight personnel **See also:** CSA, DCSA

CUI
Stands for: *Controlled unclassified information*

Information the Government creates or possesses, or that a contractor creates or possesses for it, that a law, regulation or Government-wide policy requires to be protected or dissemination-controlled, but that is not classified. The NISPOM touches CUI only where a classified contract also carries CUI terms; the rules themselves are in 32 CFR Part 2002 and the contract.

Authority: 32 CFR §117.3; 32 CFR §117.15(l); 32 CFR Part 2002 **On this site:** Export control and CUI news **See also:** CMMC, DFARS 252.204-7012

CV
Stands for: *Continuous vetting*

The Trusted Workforce 2.0 replacement for periodic reinvestigations: automated record checks, including FBI Rap Back, run throughout a person's period of eligibility, and alerts are resolved as they arise. Cleared contractor employees are enrolled through DCSA, and the rule still requires them to follow CSA guidance on reinvestigation and continuous evaluation or vetting.

Authority: 32 CFR §117.10(b)(5); DCSA: NISP contractor continuous vetting **On this site:** Continuous vetting updates · Rap Back **See also:** Continuous evaluation (CE), Trusted Workforce 2.0 (TW 2.0), Rap Back

D

DCSA
Stands for: *Defense Counterintelligence and Security Agency*

The DoD agency that administers the NISP for the Department of Defense and for the agencies that have security-service agreements with it: it is the DoD cognizant security office, grants facility clearances, oversees cleared facilities through its Industrial Security Representatives and conducts most Federal background investigations. It was the Defense Security Service (DSS) until 2020.

Authority: 32 CFR §117.6(b); DCSA: NISP oversight **On this site:** Facility clearance process map · DCSA support routes **See also:** CSO, ISR

DD Form 254
Form title: *Contract Security Classification Specification*

The form a GCA issues with a classified contract, and a prime contractor issues to each classified subcontractor, that tells the contractor the clearance and safeguarding levels required, the categories of information it will access and the classification guidance for the work. A classified contract that arrives without one should be raised with the GCA.

Authority: 32 CFR §117.13(d); 32 CFR §117.17(a)(1)(i); DD Form 254 and instructions (WHS) **On this site:** DD Form 254, item by item · DD-254 Interactive **See also:** GCA, Classified contract

DD Form 441

Form title: *Department of Defense Security Agreement*

The agreement a company signs with the Government on the way to an FCL, binding it to the NISPOM and allowing Government review of its security program; DD Form 441-1 is the appendix that adds branch offices and divisions. DCSA dates the form when it issues the FCL, and the contractor keeps the original for as long as the FCL lasts.

Authority: 32 CFR §117.9(p); DCSA job aid: DD 441; DD Form 441 (WHS) **On this site:** FCL business documents and forms · FCL issued

Derivative classification

Incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the new material to match its source or the classification guide. Contractor employees who do it need initial and refresher training; copying an existing document is not derivative classification.

Authority: 32 CFR §117.3; 32 CFR §117.13(b); 32 CFR §117.12(h) **On this site:** DD Form 254 item 13 **See also:** OCA

DFARS 252.204-7012

In full: *Safeguarding Covered Defense Information and Cyber Incident Reporting*

The DoD contract clause that requires contractors to protect covered defense information on their unclassified systems to NIST SP 800-171 and to report cyber incidents to DoD within 72 hours. For cleared defense contractors, §117.8(f) ties the NISPOM's own cyber-incident report to this clause.

Authority: DFARS 252.204-7012; 32 CFR §117.8(f) **On this site:** Cyber incident reports **See also:** CDC, CMMC, CUI

DISS

Stands for: *Defense Information System for Security*

The DoD system of record for personnel security, in which FSOs use the Joint Verification System (JVS) to verify eligibility, record access, briefings and debriefings, submit incident reports and manage their cleared population. It replaced JPAS in 2021, and DCSA is moving its functions into NBIS over time.

Authority: DCSA: Guidance for DISS management (January 2025) **On this site:** DISS transition notes · DCSA systems support **See also:** NBIS, JPAS

DOHA

Stands for: *Defense Office of Hearings and Appeals*

The DoD office whose Administrative Judges hear and decide industrial security clearance cases that a Statement of Reasons response did not resolve, and whose Appeal Board reviews those decisions. Its industrial decisions are published with names removed, and they are what the Adjudication Atlas indexes.

Authority: DoD Directive 5220.6, Defense Industrial Personnel Security Clearance Review Program; DOHA industrial security clearance decisions **On this site:** Adjudication Atlas · DOHA case status **See also:** SOR, Adjudicative guidelines

E

eApp

Stands for: *Electronic Application*

The NBIS module where an applicant completes the SF 86, SF 85P or SF 85 after the security office initiates the request; it replaced e-QIP. The FSO reviews the completed SF 86 only for adequacy and completeness and may not use its contents for anything else.

Authority: 32 CFR §117.10(d); DCSA ISL 2024-02, e-QIP to eApp **On this site:** Request and submission · KMP clearances **See also:** NBIS, e-QIP, SF 86

ECP

Stands for: *Electronic communications plan*

A CSA-approved plan, required of companies under FOCI mitigation, that shows the technical and logical separation of the cleared company's electronic communications and networks from its foreign parent or affiliates. It is tailored to the company's operations and reviewed with the rest of the mitigation agreement.

Authority: 32 CFR §117.11(h)(2) **On this site:** FOCI mitigation compared **See also:** TCP, FOCI

Eligibility

The CSA's determination, under SEAD 4, that a person may be given access to classified information at a level; it is what most people mean by a security clearance. Eligibility is not access: access also needs a need-to-know and a signed nondisclosure agreement, and is granted by the employer for the defined work.

Authority: 32 CFR §117.10(a) **On this site:** Who decides eligibility and access · Access and lifecycle **See also:** Access, PCL, SEAD 4

Entity eligibility determination

The rule's name for the CSA's assessment that a company is eligible for access to classified information at a level and all lower levels; some CSAs, DoD among them, call the favorable result an FCL. It can be broad or limited to particular contracts, agencies or circumstances.

Authority: 32 CFR §117.3; 32 CFR §117.9 **On this site:** Facility clearance process map **See also:** FCL

Entity Vetting (EV)

The DCSA office responsible for facility clearances and FOCI. From October 1, 2026 it processes the changed-condition packages that companies submit through NISS and tells the assigned ISR when a package is complete.

Authority: DCSA Industry Stakeholder Engagement, October 6, 2026 **On this site:** Changed-condition routing · October 2026 operational update **See also:** Changed condition, NISS

e-QIP RETIRED

Stands for: *Electronic Questionnaires for Investigations Processing*

OPM's former online system for completing the SF 86 and the other investigative questionnaires. It has been retired: applicants now use eApp in NBIS, which is why §117.10(d) speaks of e-QIP "or its successor system".

Authority: 32 CFR §117.10(d); DCSA ISL 2024-02, e-QIP to eApp **On this site:** Request and submission **See also:** eApp, NBIS

F

Facility
A plant, laboratory, office, college, university or commercial structure, with its associated warehouses, storage areas, utilities and components, that forms one operating entity by function and location. A company with several such locations is a multiple facility organization, and each cleared location has its own FCL.

Authority: 32 CFR §117.3 **On this site:** If your company is structured differently **See also:** MFO, FCL

FCL
Stands for: *Facility (security) clearance*

The administrative determination that a company is eligible, from a security standpoint, for access to classified information at a level and all lower levels. A company cannot apply for its own: a GCA or a cleared prime contractor sponsors it, and the FCL does not by itself authorize storing classified material at the site.

Authority: 32 CFR §117.3; 32 CFR §117.9 **On this site:** Facility clearance process map · FCL readiness check **See also:** Entity eligibility determination, Possessing and non-possessing facility, KMP

FGI
Stands for: *Foreign government information*

Information a foreign government or international organization provides to the United States with the expectation that it be kept in confidence, or that is produced jointly under such an arrangement. It is protected as classified at the equivalent U.S. level and has its own box on the DD Form 254.

Authority: 32 CFR §117.3; 32 CFR §117.19(c) **On this site:** DD Form 254 item 10 **See also:** NATO

FOCI
Stands for: *Foreign ownership, control, or influence*

A company is under FOCI when a foreign interest has the power, directly or indirectly, to direct or decide matters affecting its management or operations in a way that could result in unauthorized access to classified information or harm classified contract performance. DCSA decides, from the SF 328 and other information, whether FOCI exists and what mitigation is needed before an FCL can be granted.

Authority: 32 CFR §117.3; 32 CFR §117.11 **On this site:** FOCI mitigation compared · SF 328 guide · FOCI in the FCL process **See also:** SF 328, Board resolution, SCA, SSA, Voting trust and proxy agreement (VT, PA)

FSO
Stands for: *Facility security officer*

The U.S.-citizen employee the SMO appoints in writing to supervise and direct the company's security measures under the NISPOM. The FSO must be cleared to the FCL level, be on the KMP list and complete the training the CSA sets; the same person may also serve as ITPSO.

Authority: 32 CFR §117.7(b)(3); 32 CFR §117.3; 32 CFR §117.12(d) **On this site:** KMP clearances · Hiring an FSO consultant **See also:** KMP, SMO, ITPSO

G

GCA
Stands for: *Government contracting activity*

The element of an agency with delegated authority over acquisition: the customer that issues the DD Form 254, sponsors a company for an FCL and owns the classification guidance for its contracts. A foreign government can also be a GCA.

Authority: 32 CFR §117.3; 32 CFR §117.13(d) **On this site:** DD Form 254 guide · Who decides eligibility and access **See also:** DD Form 254

GSC
Stands for: *Government security committee*

The permanent committee of the board of directors that a company under a voting trust, proxy agreement, SSA or SCA must establish to oversee compliance with the FOCI mitigation agreement. Its members are the trustees, proxy holders or outside directors and the cleared officer-directors; the FSO is its principal advisor, attends its meetings and works under its authority.

Authority: 32 CFR §117.11(g) **On this site:** FOCI mitigation compared **See also:** SSA, SCA

H

HOF
Stands for: *Home office facility*

The headquarters location of a multiple facility organization. The home office must hold an FCL at least as high as any other cleared facility in the organization, and DCSA decides which branch offices need and qualify for their own.

Authority: 32 CFR §117.3; 32 CFR §117.9(i) **On this site:** If your company is structured differently **See also:** MFO

I

Insider threat program
The program every cleared contractor must establish to gather, integrate and report information that may indicate an insider threat: the risk that someone with authorized access will use it, wittingly or not, to harm national security. The ITPSO runs it, all cleared employees receive insider threat awareness training, and the self-inspection covers it.

Authority: 32 CFR §117.7(d); 32 CFR §117.12(g); 32 CFR §117.3 **On this site:** Insider threat program tools **See also:** ITPSO

Interim (temporary) eligibility
Eligibility the CSA may grant while an investigation is still open, when there is no adverse information that calls the applicant's trustworthiness into question; SEAD 8 now calls it temporary eligibility. A company can likewise receive an interim FCL, which carries the same access limits.

Authority: 32 CFR §117.10(l); 32 CFR §117.9(h); SEAD 8, Temporary Eligibility **On this site:** Investigation and adjudication · FCL issued **See also:** SEAD 8

ISL
Stands for: *Industrial Security Letter*

A numbered letter DCSA issues to clarify or add detail to NISPOM requirements for cleared industry. ISLs supplement the rule rather than replace it; ISL 2021-02, for example, carries the SEAD 3 reporting details for industry.

Authority: DCSA: NISP tools and resources **On this site:** Active ISLs in the guidance library · ISL 2021-02 additions **See also:** VOI, SEAD 3

ISOO
Stands for: *Information Security Oversight Office*

The office within the National Archives that oversees the Government-wide classification system and the NISP, issues the NISP implementing directive (32 CFR Part 2004) and chairs the NISPPAC. Contractors report redundant or duplicative security reviews to it.

Authority: 32 CFR §117.6(i); 32 CFR §117.8(g); 32 CFR Part 2004 **See also:** NISPPAC, NISP

ISP
Stands for: *Investigative service provider*

The agency that conducts a background investigation; for cleared industry and most of the executive branch that is DCSA. The ISP investigates and resolves coverage gaps, then hands the completed investigation to the adjudicating authority.

Authority: ODNI Federal Personnel Vetting Guidelines **On this site:** Investigation and adjudication

ISR
Stands for: *Industrial Security Representative*

The DCSA field representative assigned to a cleared facility: the FSO's main point of contact, who holds the initial orientation after an FCL is granted, conducts the recurring security reviews and answers facility-specific questions. Non-possessing facilities may be overseen by NAESOC instead.

Authority: 32 CFR §117.7(h)(1) **On this site:** Prepare for DCSA oversight · Receiving DCSA oversight personnel · Security reviews **See also:** Security review, NAESOC

ISSM
Stands for: *Information system security manager*

The employee a contractor must appoint when it processes classified information on an information system at its facility, cleared to the highest level processed, who runs the information system security program and certifies the system security plan (SSP) to the CSA. The ISSM may delegate day-to-day duties to an information systems security officer (ISSO).

Authority: 32 CFR §117.7(b)(5); 32 CFR §117.18(c)(2) **On this site:** DD Form 254 item 11

ITAR
Stands for: *International Traffic in Arms Regulations*

The State Department regulations (22 CFR Parts 120 to 130) that control the export of defense articles, defense services and related technical data, including their disclosure to foreign persons in the United States. Export control is separate from classification: an export authorization is needed before classified or export-controlled information goes to a foreign interest, and a TCP controls foreign-national access at the facility.

Authority: 32 CFR §117.19(b); 22 CFR Subchapter M **On this site:** Export control and CUI news **See also:** TCP

ITPSO
Stands for: *Insider threat program senior official*

The cleared employee the SMO appoints in writing to establish and run the company's insider threat program. The ITPSO may be the FSO; if not, the ITPSO must make the FSO an integral member of the program, and an entity family may appoint one ITPSO for all its cleared facilities.

Authority: 32 CFR §117.7(b)(4); 32 CFR §117.3 **On this site:** Insider threat program tools · KMP clearances **See also:** Insider threat program, KMP

J

JPAS RETIRED
Stands for: *Joint Personnel Adjudication System*

DoD's former personnel security system of record for industry and the Department. It was retired in 2021 and replaced by DISS; older guidance that says to record something in JPAS now means DISS.

Authority: DCSA: Guidance for DISS management (January 2025) **On this site:** DISS transition notes **See also:** DISS

K

KMP
Stands for: *Key management personnel*

The SMO, FSO, ITPSO and every other official who holds a majority interest in the company or can influence or decide matters affecting its management, operations or classified contract performance. Each must be cleared to the FCL level or be formally excluded from classified information by a board resolution, and changes to the KMP list are reported to DCSA.

Authority: 32 CFR §117.3; 32 CFR §117.7(c); 32 CFR §117.8(c)(7)(iii) **On this site:** KMP clearances **See also:** SMO, FSO, ITPSO

L

LAA

Stands for: *Limited access authorization*

Access to Confidential or Secret information granted, for compelling reasons, to a non-U.S. citizen who needs only limited access in regular duties. It is never valid for Top Secret, Restricted Data, COMSEC, intelligence, NATO or third-country information, and the contractor reports when the need for it ends.

Authority: 32 CFR §117.3; 32 CFR §117.10(k) **On this site:** LAA reports

LOD

Stands for: *Letter of Denial*

The notice that eligibility has been denied (LOD) or revoked (LOR) after the response to a Statement of Reasons did not resolve the security concerns, with the person's appeal rights. For industry applicants an unresolved SOR goes to DOHA for decision instead, so an FSO more often sees the LOI and SOR stage in DISS.

Authority: DoD Manual 5200.02, Procedures for the DoD Personnel Security Program **On this site:** Investigation and adjudication **See also:** LOI, SOR, DOHA

LOI

Stands for: *Letter of Intent*

The letter in which the adjudicator states its intent to deny or revoke eligibility; it comes with the Statement of Reasons (SOR) that lists the concerns, and the person has a set time to respond in writing. For a contractor employee the package is sent through the FSO for delivery, and the LOI is a pending action, not a final decision.

Authority: DoD Manual 5200.02, Procedures for the DoD Personnel Security Program; DoD Directive 5220.6, Defense Industrial Personnel Security Clearance Review Program **On this site:** Investigation and adjudication **See also:** SOR, LOD, DOHA

M

MFO

Stands for: *Multiple facility organization*

A single legal entity, such as a corporation or partnership, made up of two or more facilities. Its home office must be cleared at least as high as any of its other cleared facilities, and DCSA decides which branch offices need and qualify for their own FCL.

Authority: 32 CFR §117.3; 32 CFR §117.9(i) **On this site:** If your company is structured differently **See also:** HOF, Facility

N

NAESOC

Stands for: *National Access Elsewhere Security Oversight Center*

The DCSA center that oversees cleared contractors whose employees work with classified information only at Government or other cleared sites and who hold none at their own facility. For those non-possessing facilities it takes the place of the local field office and its ISR.

Authority: DCSA: NAESOC resources **On this site:** Changed-condition routing **See also:** Possessing and non-possessing facility, ISR

NATO

Stands for: *North Atlantic Treaty Organization*

NATO information is information bearing NATO markings, which may be released outside NATO and its member nations only with NATO's authority; it has its own briefings, markings, registry controls and its own box on the DD Form 254. A contractor needs a NATO Facility Security Clearance Certificate (FSCC), issued by the CSA on the strength of its FCL, to negotiate or perform on a NATO classified contract.

Authority: 32 CFR §117.3; 32 CFR §117.19(g) **On this site:** DD Form 254 item 10 **See also:** FGI

NBIS

Stands for: *National Background Investigation Services*

DCSA's information technology platform for the end-to-end personnel vetting process, built to replace legacy systems, including e-QIP (now eApp inside NBIS) and, over time, DISS. DCSA has announced and revised transition dates more than once, so follow its current notices for which system to use for what.

Authority: 32 CFR §117.10(d) **On this site:** DISS transition notes · Applicant and systems support **See also:** eApp, DISS

NDA

Stands for: *Nondisclosure agreement*

The agreement between the U.S. Government and a person found eligible for access, signed before any access to classified information; in industry it is the SF 312, Classified Information Nondisclosure Agreement. An employee's refusal to sign it is reported to the CSA, and no access may be granted without it.

Authority: 32 CFR §117.10(g); 32 CFR §117.8(c)(6) **On this site:** Access and lifecycle · Refusal to sign the SF 312 **See also:** SF 312

Need-to-know

A determination by an authorized holder of classified information that a prospective recipient needs it to perform tasks essential to a classified contract or program. Eligibility alone never justifies access; need-to-know is decided for each disclosure.

Authority: 32 CFR §117.3; 32 CFR §117.10(a)(1)(iii) **On this site:** Access and lifecycle **See also:** Access

NID

Stands for: *National interest determination*

The CSA's determination that letting a company under a special security agreement have access to proscribed information is consistent with national security; for SCI, Restricted Data and COMSEC the controlling agency (ODNI, DOE or NSA) must concur. It applies only to SSA companies, and the law exempts some NTIB companies from it.

Authority: 32 CFR §117.11(d)(2)(iii); DCSA: National interest determinations **On this site:** National interest determinations **See also:** SSA, Proscribed information

NISP

Stands for: *National Industrial Security Program*

The single program, created by Executive Order 12829 in 1993, under which the executive branch protects classified information released to contractors, licensees and grantees. ISOO's directive in 32 CFR Part 2004 governs it, the five CSAs run it, and the NISPOM sets the requirements contractors follow.

Authority: E.O. 12829, National Industrial Security Program; 32 CFR Part 2004; 32 CFR §117.1 **On this site:** Facility clearance process map **See also:** NISPOM, CSA

NISPOM

Stands for: *National Industrial Security Program Operating Manual*

The requirements cleared contractors follow to protect classified information. Since February 24, 2021 it has been a Federal regulation, 32 CFR Part 117, which replaced the DoD manual (DoD 5220.22-M) of the same name; contractors had until August 24, 2021 to comply, and section numbers on this site (§117.8, for example) refer to it.

Authority: 32 CFR Part 117; DCSA: 32 CFR Part 117 NISPOM rule **On this site:** Key dates for cleared industry **See also:** NISP, ISL

NISPPAC

Stands for: *National Industrial Security Program Policy Advisory Committee*

The advisory committee that E.O. 12829 created under ISOO, with Government and industry members, where NISP policy and performance are discussed. DCSA briefs its personnel vetting processing times there each quarter.

Authority: E.O. 12829, section 103 **On this site:** Processing times **See also:** ISOO

NISS

Stands for: *National Industrial Security System*

DCSA's system of record for facility clearances. Sponsors submit FCL sponsorship requests and verify existing FCLs there, companies submit their FCL packages and changed-condition reports, and DCSA records the results of security reviews.

Authority: DCSA: Facility clearances **On this site:** FCL sponsorship · Changed-condition routing **See also:** FCL, Changed condition

O

OCA

Stands for: *Original classification authority*

A Government official authorized in writing to decide, in the first instance, that information must be classified. Contractors never classify originally; they classify derivatively from an OCA's guidance, carried to them by the DD Form 254 and the classification guide.

Authority: 32 CFR §117.3; 32 CFR §117.13(a) **On this site:** DD Form 254 item 13 **See also:** Derivative classification

OPSEC

Stands for: *Operations security*

The process of identifying critical information and the unclassified indicators that could reveal it, then protecting them from an adversary's view. A contract imposes OPSEC requirements on a contractor through the DD Form 254; the NISPOM itself does not define the term.

Authority: DoD Directive 5205.02E, DoD Operations Security (OPSEC) Program **On this site:** DD Form 254 item 11

P

PCL

Stands for: *Personnel (security) clearance*

The administrative determination that an individual is eligible, from a security standpoint, for access to classified information at a level and below. The CSA makes it under SEAD 4; the contractor requests it only for employees and consultants who need access to perform on a classified contract.

Authority: 32 CFR §117.3; 32 CFR §117.10 **On this site:** Security clearance process map **See also:** Eligibility, FCL

Possessing and non-possessing facility

A possessing facility has CSA-approved safeguarding capability and stores classified material on site; a non-possessing facility's employees work with classified information only at Government or other cleared contractor locations. The FCL and the storage approval are separate determinations, and the DD Form 254 records them separately in items 1a and 1b.

Authority: 32 CFR §117.9(a)(3); 32 CFR §117.9(a)(6); 32 CFR §117.15 **On this site:** FCL issued · DD Form 254 item 1 **See also:** FCL, Closed area, NAESOC

Prime contractor and subcontractor

The prime contractor holds the contract from the GCA; a subcontractor supplies goods or services to it under a subcontract. Before releasing classified information to a subcontractor the prime must confirm its FCL (or sponsor one), issue it a DD Form 254 and, where the GCA requires, obtain approval; subcontractors report certain conditions to the prime as well as to the CSA.

Authority: 32 CFR §117.3; 32 CFR §117.17; 32 CFR §117.8(c)(10) **On this site:** Subcontracts on the DD Form 254 · Prime and subcontractor reports

Proscribed information

Five categories the rule singles out: Top Secret information, COMSEC (other than unkeyed controlled cryptographic items), Restricted Data, SAP information and SCI. A company under a special security agreement needs a national interest determination before it may access any of them.

Authority: 32 CFR §117.3; 32 CFR §117.11(d)(2)(iii) **On this site:** National interest determinations **See also:** NID, SSA

PSMO-I

Stands for: *Personnel Security Management Office for Industry*

The DCSA office that handles industry personnel security actions in DISS: processing clearance requests, reviewing incident reports against the thresholds for suspending eligibility, and passing cases to adjudication. Facility matters go to the ISR, not to PSMO-I.

Authority: DCSA Industry Stakeholder Engagement, October 6, 2026 **On this site:** Where reports go · DCSA support routes **See also:** DISS, ISR

Public Trust position

A Federal position of moderate or high risk to the integrity or efficiency of the service that does not require access to classified information. It takes a Tier 2 or Tier 4 investigation on the SF 85P and a suitability or fitness determination rather than a security clearance, and its reporting rules come from the agency, not the NISPOM.

Authority: 5 CFR 731.106 **On this site:** Public Trust reporting · Investigation tiers **See also:** SF 85P, Tier 3 and Tier 5 (T3, T5)

PVQ

Stands for: *Personnel Vetting Questionnaire*

The common questionnaire designed under Trusted Workforce 2.0 to replace the SF 85, SF 85P and SF 86 with one form. DCSA's October 2026 briefing described limited production use, not a general rollout; applicants complete whichever form their case assigns.

Authority: DCSA Industry Stakeholder Engagement, October 6, 2026 **On this site:** Continuous vetting updates **See also:** SF 86, Trusted Workforce 2.0 (TW 2.0)

R

Rap Back

The FBI service that notifies a subscribing agency when new criminal-history activity is recorded against the fingerprints of an enrolled person. DCSA uses it as one of the automated inputs to continuous vetting, and new enrollments bring Privacy Act notices into onboarding.

Authority: DCSA Industry Stakeholder Engagement, October 6, 2026 **On this site:** Rap Back notices and onboarding **See also:** CV

Reciprocity

The rule that one agency accepts another's current investigation, eligibility determination or FCL at the same or a higher level instead of repeating it, unless a specified exception applies. SEAD 7 governs it for people; §117.9(b) applies it to entity eligibility determinations between CSAs.

Authority: 32 CFR §117.10(h); 32 CFR §117.9(b); SEAD 7, Reciprocity of Background Investigations and National Security Adjudications **On this site:** Request and submission · FCL sponsorship **See also:** SEAD 7

Restricted Data (RD) and Formerly Restricted Data (FRD)

Restricted Data is information about the design, manufacture or use of atomic weapons, the production of special nuclear material or its use in producing energy, classified under the Atomic Energy Act rather than an executive order; Formerly Restricted Data has been moved out of that category by joint DOE and DoD determination because it relates mainly to the military use of atomic weapons. DOE sets the protection rules, and Restricted Data is proscribed information.

Authority: 32 CFR §117.3; 32 CFR §117.23(e) **On this site:** DD Form 254 item 10 · National interest determinations **See also:** CNWDI, Proscribed information

S

SAP

Stands for: *Special access program*

A program established under E.O. 13526 to control access to and protect particularly sensitive classified information beyond what Top Secret, Secret or Confidential normally requires. SAP access is approved separately from the clearance, SAP information is proscribed information, and a SAP contract's security requirements come from the program's own rules.

Authority: 32 CFR §117.3; 32 CFR §117.23(d) **On this site:** SCI and SAP access · DD Form 254 item 10 **See also:** SCI, Proscribed information

SCA

Stands for: *Security control agreement*

The FOCI mitigation agreement used when a foreign interest does not effectively own or control the company but is entitled to representation on its board. The company stays under U.S. control, and the SCA places no restriction on the classified information it may access, so no national interest determination is needed.

Authority: 32 CFR §117.11(d)(2)(ii) **On this site:** FOCI mitigation compared **See also:** SSA, GSC, FOCI

SCI

Stands for: *Sensitive compartmented information*

Classified national intelligence about or derived from intelligence sources, methods or analytical processes that must be handled within formal access control systems the Director of National Intelligence establishes. SCI access is approved separately from a Top Secret clearance, is held in an accredited SCIF, and is proscribed information; DCSA does not oversee it.

Authority: 32 CFR §117.3; 32 CFR §117.23(b) **On this site:** SCI and SAP access · DD Form 254 item 10 **See also:** SAP, Proscribed information

SEAD

Stands for: *Security Executive Agent Directive*

A directive the Director of National Intelligence issues as Security Executive Agent for the Government-wide personnel security system. The NISPOM makes several of them binding on cleared industry: SEAD 3 (reporting), SEAD 4 (adjudicative guidelines), SEAD 6 (continuous evaluation), SEAD 7 (reciprocity) and SEAD 8 (temporary eligibility).

Authority: 32 CFR §117.3; 32 CFR §117.8(a) **On this site:** Personnel reporting requirements **See also:** SEAD 3, SEAD 4, SEAD 6, SEAD 7, SEAD 8

SEAD 3

In full: *Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position*

The directive that sets what cleared people must report about themselves (unofficial foreign travel, foreign contacts, financial and conduct matters, among others) and what they must report about others. It took effect June 12, 2017; cleared industry has reported under it through the NISPOM rule since August 24, 2021, with DCSA's ISL 2021-02 adding detail.

Authority: SEAD 3; 32 CFR §117.8(a) **On this site:** Cleared industry reporting · Government and service member reporting **See also:** ISL, Adverse information

SEAD 4

In full: *National Security Adjudicative Guidelines*

The directive that sets the thirteen adjudicative guidelines and the whole-person standard adjudicators apply when deciding eligibility for access to classified information or a sensitive position. It took effect June 8, 2017, and the CSA decides contractor employees' eligibility under it.

Authority: SEAD 4; 32 CFR §117.10(a)(2) **On this site:** DOHA decisions by guideline · Adjudication Atlas **See also:** Adjudicative guidelines, DOHA

SEAD 6

In full: *Continuous Evaluation*

The 2018 directive that established continuous evaluation of people holding eligibility, through automated records checks between reinvestigations; the NISPOM's definition of continuous evaluation points to it. Trusted Workforce 2.0 carries the approach forward as continuous vetting.

Authority: SEAD 6, Continuous Evaluation; 32 CFR §117.3 **On this site:** Continuous vetting updates **See also:** Continuous evaluation (CE), CV

SEAD 7

In full: *Reciprocity of Background Investigations and National Security Adjudications*

The 2018 directive that requires agencies to accept each other's background investigations and eligibility determinations at the same or a higher level, with only the exceptions it lists, rather than investigate again. The NISPOM applies the same principle to contractor employees who were cleared or investigated elsewhere.

Authority: SEAD 7, Reciprocity of Background Investigations and National Security Adjudications; 32 CFR §117.10(h) **On this site:** Request and submission **See also:** Reciprocity

SEAD 8

In full: *Temporary Eligibility*

The directive that governs temporary eligibility, the term that replaced interim clearance, granted while an investigation is still under way. The NISPOM lets the CSA grant it to applicants for Top Secret, Secret or Confidential when nothing adverse calls their trustworthiness into question.

Authority: SEAD 8; 32 CFR §117.10(l) **On this site:** Investigation and adjudication **See also:** Interim (temporary) eligibility

Security in depth

The CSA's determination that a contractor's security program consists of layered and complementary controls, such as perimeter fences, access controls, intrusion detection, guard patrols and video monitoring, sufficient to deter and detect unauthorized entry and movement. It can reduce the supplemental protection open storage areas and containers would otherwise need.

Authority: 32 CFR §117.3; 32 CFR §117.15 **See also:** Closed area

Security review

DCSA's recurring oversight review of a cleared contractor's security program, announced or unannounced, at a frequency it sets by risk; taking part is a condition of keeping the FCL. Each review ends with a rating from DCSA's rating tools, and findings are tracked to resolution.

Authority: 32 CFR §117.7(h)(1); DCSA: Security review rating process **On this site:** Security reviews and corrective actions · Receiving DCSA oversight personnel **See also:** Self-inspection, ISR

Security training (initial briefing, refresher, debriefing)

Every cleared employee gets an initial security briefing before access, refresher training every twelve months and a debriefing when access ends; the FSO and others with security duties take training the CSA sets, and the ITPSO sees that everyone completes insider threat training. The contractor records all of it.

Authority: 32 CFR §117.12(e); 32 CFR §117.12(k); 32 CFR §117.12(l); 32 CFR §117.12(g) **On this site:** Training and compliance calendar · Keeping the FCL **See also:** CDSE

Security violation

A failure to follow the rule's policies and procedures that could reasonably result in the loss or compromise of classified information. Violations are investigated and, when they involve loss, compromise or suspected compromise, reported to the CSA; the final report states the action taken against a responsible employee whose violation involved deliberate disregard, negligence with classified material or a recurring pattern of carelessness.

Authority: 32 CFR §117.3; 32 CFR §117.8(e) **On this site:** Individual culpability reports **See also:** Compromise

Self-inspection

The contractor's own formal review of its security program, at least annually and at intervals consistent with risk, covering classified activity, information, information systems, the overall program and the insider threat program. A written report records findings and their resolution, and the SMO certifies to the CSA each year that it was done and the other KMP briefed.

Authority: 32 CFR §117.7(h)(2); DCSA: Self-Inspection Handbook for NISP contractors **On this site:** Security reviews and corrective actions · ITP self-inspection tool **See also:** Security review, SMO

SF 312

Form title: *Classified Information Nondisclosure Agreement*

The nondisclosure agreement between the U.S. Government and a person found eligible for access, signed and witnessed before any access to classified information; its obligations continue after access ends. A refusal to sign is reported to the CSA, and the signed form is kept for the period the Government requires.

Authority: 32 CFR §117.10(g); SF 312 (GSA forms library) **On this site:** Access and lifecycle · Refusal to sign the SF 312 **See also:** NDA

SF 328

Form title: *Certificate Pertaining to Foreign Interests*

The form on which a company answers nine questions about foreign ownership, control and influence, under penalty of 18 U.S.C. §1001, during FCL processing and again whenever the answers change materially. Any Yes needs supporting documentation and leads DCSA to a FOCI determination.

Authority: 32 CFR §117.11(c); 32 CFR §117.8(c)(7)(v); SF 328 (GSA forms library) **On this site:** SF 328, question by question · FOCI mitigation compared **See also:** FOCI, CFIUS

SF 85P

Form title: *Questionnaire for Public Trust Positions*

The OPM questionnaire for Tier 2 and Tier 4 investigations of moderate- and high-risk Public Trust positions, completed in eApp. It supports a suitability or fitness determination, not a security clearance; the SF 85 serves low-risk positions and the SF 86 national security positions.

Authority: OPM Federal investigation forms **On this site:** Public Trust reporting · Investigation tiers **See also:** Public Trust position, SF 86

SF 86

Form title: *Questionnaire for National Security Positions*

The questionnaire an applicant completes in eApp for a Tier 3 or Tier 5 investigation, the basis of a Confidential, Secret or Top Secret eligibility determination. The FSO or a designated reviewer checks it only for adequacy and completeness, tells the employee so in writing and may not use its contents for any other purpose.

Authority: 32 CFR §117.10(d); OPM Federal investigation forms **On this site:** Request and submission · Investigation tiers **See also:** eApp, Tier 3 and Tier 5 (T3, T5)

SMO

Stands for: *Senior management official*

The company employee with ultimate authority over the facility's operations and the authority to direct whatever is needed to safeguard classified information, who stays accountable for the security program without delegating that accountability. The SMO appoints the FSO and ITPSO in writing and certifies the annual self-inspection to the CSA.

Authority: 32 CFR §117.3; 32 CFR §117.7(b)(2); 32 CFR §117.7(h)(2)(iii) **On this site:** KMP clearances **See also:** KMP, FSO, Self-inspection

SOR

Stands for: *Statement of Reasons*

The written statement of the security concerns, organized by SEAD 4 guideline, that accompanies a notice of intent to deny or revoke a person's eligibility, and which the person answers in writing within the time allowed. DCSA also issues a Statement of Reasons before denying or revoking a company's FCL. For a contractor employee, an unresolved SOR goes to DOHA for a hearing or a decision on the written record.

Authority: DoD Directive 5220.6, Defense Industrial Personnel Security Clearance Review Program; 32 CFR §117.9 **On this site:** Adjudication Atlas · DCSA review and adjudication **See also:** LOI, DOHA, Adjudicative guidelines

SPP

Stands for: *Standard practice procedures*

The contractor's written procedures implementing the NISPOM's requirements for its own operations and involvement with classified information, prepared when the CSA finds them necessary to rule out loss or compromise. ISL 2021-02 expects the SEAD 3 reporting procedures to be written down there.

Authority: 32 CFR §117.3; 32 CFR §117.7(e) **On this site:** ISL 2021-02 additions · Insider threat program plan builder

SSA

Stands for: *Special security agreement*

The FOCI mitigation agreement used when a foreign interest effectively owns or controls the company: it allows the foreign owner representation on the board under negotiated controls, with outside directors, a government security committee and plans for technology and electronic communications. An SSA company needs a national interest determination before it may access proscribed information.

Authority: 32 CFR §117.11(d)(2)(iii) **On this site:** FOCI mitigation compared · National interest determinations **See also:** NID, GSC, SCA, Voting trust and proxy agreement (VT, PA)

STEPP

Stands for: *Security Training, Education and Professionalization Portal*

CDSE's learning management portal, where cleared industry takes the FSO curriculum, insider threat and other security courses and keeps completion records. DCSA's briefings and job aids on system changes are often published as STEPP courses or demonstrations.

Authority: CDSE FSO Toolkit **On this site:** October 2026 operational update **See also:** CDSE

SWFT

Stands for: *Secure Web Fingerprint Transmission*

DCSA's system for submitting electronic fingerprints for background investigations; paper fingerprint cards are no longer accepted for industry. A company without its own enrollment equipment uses an approved provider that submits through SWFT.

Authority: 32 CFR §117.10(e); DCSA: Fingerprints **On this site:** KMP clearances · FCL readiness check: KMP

T

TCP

Stands for: *Technology control plan*

A CSA-approved plan that controls foreign nationals' access to classified and export-controlled information at a cleared facility: required of companies under a voting trust, proxy agreement, SSA or SCA, and whenever foreign nationals are employed at or make long-term visits to a cleared facility, unless existing procedures are adequate. A sample is available from the CSA.

Authority: 32 CFR §117.11(h)(1); 32 CFR §117.19(e)(4)(v) **On this site:** FOCI mitigation compared **See also:** ECP, ITAR

Tier 3 and Tier 5 (T3, T5)

The investigation tiers of the Federal Investigative Standards: Tier 3, on the SF 86, supports Confidential and Secret eligibility; Tier 5, also on the SF 86, supports Top Secret and SCI; Tiers 1, 2 and 4 serve low-risk and Public Trust positions. An investigation supports a determination and does not itself grant eligibility or access.

Authority: ODNI Federal Personnel Vetting Guidelines; DCSA: Case types and forms **On this site:** Position type to investigation tier · Processing times **See also:** SF 86, SF 85P

Trusted Workforce 2.0 (TW 2.0)

The Government-wide reform of personnel vetting led by the Security and Suitability Executive Agents under the Performance Accountability Council: one vetting framework for every kind of trust determination, continuous vetting in place of periodic reinvestigations, and shared systems such as NBIS. TW 1.5 was the interim stage, with five-year checks, before TW 2.0's annual checks.

Authority: Performance Accountability Council, Trusted Workforce 2.0 quarterly progress report **On this site:** Continuous vetting updates · Processing times **See also:** CV, NBIS, PVQ

V

VAL

Stands for: *Visit authorization letter*

The letter a contractor sends ahead of a classified visit to verify the visitor's clearance, when the CSA-designated database (DISS for DoD) cannot be used. It names the visitor, their clearance level, the purpose and dates of the visit and the point of contact, and the host still decides need-to-know.

Authority: 32 CFR §117.16(a)(4) **See also:** DISS, Need-to-know

VOI

Stands for: *Voice of Industry*

DCSA's monthly newsletter for cleared industry, with operational notices, system changes and reminders. It is guidance about process, not regulation; the guidance library keeps the archive of issues, and this site's reviewed products note which VOI each change came from.

Authority: DCSA: NISP tools and resources **On this site:** VOI archive in the guidance library **See also:** ISL

Voting trust and proxy agreement (VT, PA)
The strongest FOCI mitigation arrangements, which vest the voting rights of the foreign-owned stock in cleared U.S. citizens approved by the Government: under a voting trust the foreign owner transfers legal title to the trustees, under a proxy agreement only the voting rights pass to the proxy holders. Neither limits the company's access to classified information or its eligibility to compete for classified contracts.

Authority: 32 CFR §117.11(d)(2)(iv) **On this site:** Voting trust · Proxy agreement
See also: SSA, GSC, FOCI

How this glossary is kept

Definitions follow the rule's own wording in plain language, shortened but not changed in meaning. Where the NISPOM defines a term, §117.3 is cited; where a procedure gives it meaning, that paragraph is. Terms from DCSA practice, such as ISR, VOI or PSMO-I, cite DCSA's published material instead.

Sources: 32 CFR Part 117 (eCFR text current as of 2026-10-31); SEAD 3, SEAD 4 and SEAD 8; DCSA NISP tools and resources; and the official pages linked from each entry. A retired term is marked and names its replacement. The rule and the official source control where they are more specific. Not legal advice. To suggest a term or a correction, use the link in the footer.