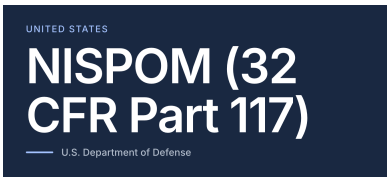
SmartSuite

Framework / Supply Chain Security / Other

National Industrial Security Program Operating Manual (NISPOM), 32 CFR Part 117

The NISPOM (32 CFR Part 117) is the DoD rule on how cleared contractors protect classified information: eligibility, FSO and ITPSO roles, insider threat, reporting, FOCI, self-inspection.



What it is

The National Industrial Security Program Operating Manual (NISPOM), codified at 32 CFR Part 117, is the Department of Defense rule that prescribes how contractors, licensees, grantees and other non-government entities protect the classified information the U.S. Government discloses to them or that they develop under classified contracts; it took effect on February 24, 2021, contractors had to implement it within six months of that date, and it replaced the manual DoD 5220.22-M as the governing text for cleared industry. The rule was published as 85 FR 83312 on December 21, 2020 and amended once, on August 19, 2021 (86 FR 46598).

At a glance

PUBLISHER
U.S. Department of Defense (rule); administered for DoD by the Defense Counterintelligence and Security Agency (DCSA)

TYPE
Regulation

VERSION
32 CFR Part 117 (85 FR 83312, December 21, 2020), as amended August 19, 2021 (86 FR 46598)

EFFECTIVE
February 24, 2021 (contractor compliance within six months)

DOMAIN
Supply Chain Security

FAMILY
Other

REGION
United States

INDUSTRY
Aerospace & Defense

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117

Why it matters

- **One rule for all five CSAs** Section 117.3 defines the CSAs as DoD, DOE, NRC, ODNI and DHS, so a contractor cleared under more than one agency works from the same codified text, supplemented by CSA guidance.
- **Named accountable officials** Section 117.7(b) requires the SMO to appoint, in writing, a U.S. citizen employee as FSO and as ITPSO, and 117.7(b)(5) an ISSM wherever classified information is processed on an information system at the facility.
- **A reporting regime with fixed triggers** Section 117.8 lists what goes to the FBI and what goes to the CSA: adverse information, suspicious contacts, changes in cleared employee status, FOCI changes on an updated SF 328, loss or compromise, and cyber incidents on classified systems.
- **FOCI handled in the rule itself** Section 117.11 requires the SF 328 Certificate Pertaining to Foreign Interests and sets the mitigation instruments, from board resolutions to security control agreements, special security agreements, voting trusts and proxy agreements.

© 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NISPOM (32 CFR Part 117)

Part 117 Requirement Library

Load sections 117.7 to 117.23 as requirements with the SMO, FSO, ITPSO or ISSM as owner, implementation status, linked procedures and the evidence a DCSA security review asks for.

KMP Roster and Exclusions

Keep the key management personnel list of 117.7(c) with each official's eligibility status, appointment letters for the FSO and ITPSO and any board exclusion resolutions, ready for the CSA.

117.8 Reporting Workflow

Route adverse information, suspicious contacts, employee status changes, loss or compromise and classified-system cyber incidents to the FSO, with the CSA or FBI submission, date and follow-up recorded.

Annual Self-Inspection

Run the 117.7 self-inspection in Internal Audit Management with scope, findings, corrective actions and the SMO's written certification, retained until the next CSA security review.

FOCI and SF 328 Changes

Track ownership, debt, board and foreign-contract changes against the last SF 328, the mitigation agreement in place and the 117.11 reporting duty when a material change occurs.

Subcontractor Flow-Down

Record each classified subcontract, the subcontractor's entity eligibility and the 117.8 duty to report conditions under which a subcontractor cannot protect classified information, in Third Party Risk Management.

Common framework mappings

CIS Controls v8.1 | CMMC 2.0 | CSA CCM v4 | ISO 27001:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | SOC 2

Official resources

32 CFR Part 117 (NISPOM) on the eCFR

The current codified text of the NISPOM rule, sections 117.1 to 117.24, kept up to date by the Office of the Federal Register.

ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117

NISPOM final rule, 85 FR 83300 (December 21, 2020)

The Federal Register rule that codified the NISPOM at 32 CFR Part 117, with its preamble, the February 24, 2021 effective date and the six-month implementation period.

federalregister.gov/documents/2020/12/21/2020-27698/national-industrial-security-program-operating-manual-nispom

32 CFR Part 117, 2025 annual edition (govinfo)

The Government Publishing Office's official annual Code of Federal Regulations text of Part 117.

govinfo.gov/app/details/CFR-2025-title32-vol1/CFR-2025-title32-vol1-part117

Frequently asked questions

What is the NISPOM, and what did 32 CFR Part 117 replace?

The National Industrial Security Program Operating Manual is the Department of Defense rule, codified at 32 CFR Part 117, that prescribes how contractors protect classified information disclosed to them or developed under classified contracts (117.1). It was published on December 21, 2020 (85 FR 83312), took effect on February 24, 2021, and replaced the manual DoD 5220.22-M; contractors had to implement it within six months, and the only amendment since, on August 19, 2021, concerned 117.1.

Who does the NISPOM apply to, and which agencies run the program?

Section 117.2 applies the rule to DoD components, all executive branch departments and agencies, and every industrial, educational, commercial or other non-government entity granted access to classified information, through every phase of a contract, agreement, license or grant. Section 117.3 names five cognizant security agencies, DoD, DOE, NRC, ODNI and DHS; for DoD and the agencies under its cognizance, DCSA is the office that determines entity eligibility, conducts security reviews and receives reports.

Which officials must a cleared contractor appoint?

Under 117.7(b) the senior management official (SMO) is accountable for the security program and appoints, in writing, a U.S. citizen employee as facility security officer (FSO) and as insider threat program senior official (ITPSO), who may be the same person. Where classified information is processed on an information system at the facility, the contractor also appoints an information system security manager (ISSM). These officials are key management personnel who must hold eligibility for access to classified information and cannot be excluded from it (117.9).

What does the NISPOM require for self-inspections and security reviews?

Section 117.7(h) requires a formal self-inspection at least annually, covering classified activity, classified information and systems, the overall program and the insider threat program, with a written report retained until the next CSA security review. The SMO certifies annually in writing to the CSA that the self-inspection was done, that other key management personnel were briefed, that corrective actions were taken and that management supports the program. The CSA's own recurring security reviews are a condition of keeping entity eligibility.

What is FOCI, and what is the SF 328?

Foreign ownership, control or influence is addressed in 117.11. An entity completes the SF 328, Certificate Pertaining to Foreign Interests, during its entity eligibility determination and again when the information changes, and 117.8 requires a report of any material FOCI change on an updated SF 328. Where FOCI exists, the CSA decides whether it can be mitigated by measures such as board resolutions, security control agreements, special security agreements, voting trusts or proxy agreements; FOCI that cannot be mitigated consistent with the national interest bars eligibility (117.9).

License included / downloadable: Yes The NISPOM is a U.S. federal regulation published free of charge in the Code of Federal Regulations and on the eCFR; the platform links to the official text.

Full framework page and mappings: smartsuite.com/frameworks/us-nispom-national-industrial-security-program-operating-manual

© 2026 SmartSuite Inc. All rights reserved.