FSO Variance Catalog

Authority-first, chronology-aware FSO reference

DCSA interpretive and operational guidance measured against 32 CFR Part 117

Catalog scope	Value
Scope	21 requirements; 0 extra-regulatory topic(s)
Sources	775 approved findings; 73 entry-history touches; 23 CFR baseline citation(s)
Cycle	2026-01
Status	Working reference. The CFR, contract, and incorporated authorities remain controlling.

1. Scope and use

This catalog states the Part 117 baseline first, then shows what DCSA interpretation and execution guidance adds. It preserves the approved guidance trail so an FSO can identify the current instruction without losing the history that explains it.

1.1 Contents

• 3.1 Administrative findings, vulnerabilities, and mitigation follow-up - § 117.7(h)(2)

• 3.2 Advertising positions requiring a Personnel Security Clearance - § 117.9(a)(9)

• 3.3 Changed-condition reporting and Entity Vetting processing - § 117.8(c)(7)

• 3.4 Classified Information Nondisclosure Agreement (SF 312) - § 117.10(g)

• 3.5 CUI training frequency — annual to biennial - § 117.12(f), § 117.18(f)

• 3.6 DCSA representative credentials and classified-visit access - § 117.16(a)(1), § 117.16(a)(3)

• 3.7 Do not search for classified information in the public domain - § 117.15(a), § 117.8(a)(1), § 117.8(d), § 117.18(b)(2)

• 3.8 Fingerprint Collection - § 117.10(e), § 117.10(b)(5)

• 3.9 FY27 security review prioritization and baseline frequency - § 117.7(h)

• 3.10 Information System Security and Commercial Cloud Services - § 117.18

• 3.11 Insider Threat Program and ITPSO Appointment - § 117.7(b)(4), § 117.7(d), § 117.12(g), § 117.18(a)(1), § 117.18(b)(4)

• 3.12 International plans and notices submission route - § 117.19(d)

• 3.13 MFO classified performance, disclosure, and DD Form 254 locations - § 117.9(i), § 117.13(d), § 117.15(h)(1), § 117.15(h)(3)

• 3.14 NAESOC oversight team verification for newly transitioned facilities - § 117.7(l)

• 3.15 Open Storage Areas (formerly Closed Areas) - § 117.15(c), § 117.15(b)

• 3.16 Reinvestigation and Continuous Vetting - § 117.10(b)(5)

• 3.17 Reporting Requirements and SEAD 3 Reportable Activities - § 117.8, § 117.7(h)(2)(i), § 117.7(h)(2)(ii), § 117.7(h)(2)(iii)

• 3.18 Security Rating Score Tool 2.0 and self-inspection alignment - § 117.7(h)(2)

• 3.19 SF-328 Certificate Pertaining to Foreign Interests — revised form - § 117.11(b), § 117.11(d)

• 3.20 Submission of the SF 86 (NBIS eApp) - § 117.10(d)

• 3.21 Verification of U.S. Citizenship - § 117.10(c)

1.2 Structure of each requirement

• What DCSA guidance adds to the rule - the operational difference between the CFR baseline and current practice.

• Regulatory text - the controlling Part 117 baseline.

• Required practice - numbered actions identify their basis as Rule, Incorporated authority, Binding DCSA supplementary procedures, or DCSA guidance.

• Matters not addressed by the regulation - operational details supplied by guidance.

• Guidance changed in the preceding year - every change in the review window, plus the immediately preceding direction when needed to show what changed.

1.3 Interpretive standard

• 32 CFR Part 117 - primary authority. The regulation controls; guidance cannot amend or contradict it.

• Industrial Security Letters - DCSA's enforceable interpretation. ISLs state how DCSA interprets or applies the CFR within their scope.

• Voice of Industry - day-to-day execution direction. VOIs provide operational direction and clarification within their scope.

Read each history oldest-to-newest. The newest applicable active guidance is the current operational direction. Recency does not displace the CFR, and later guidance controls only the people, systems, dates, and situations it addresses.

1.4 Limitations

• This document is not itself an authority and does not confer an approval.

• Source guidance is summarized, not reproduced; verify quotations and unusual facts against the source.

• A deterministic renderer can display only the approved conclusions stored in the catalog.

1.5 Acronym legend

Acronym	Meaning	Acronym	Meaning
CFR	Code of Federal Regulations	DCSA	Defense Counterintelligence and Security Agency
FSO	Facility Security Officer	ISL	Industrial Security Letter
SEAD	Security Executive Agent Directive	VOI	Voice of Industry

1.6 2026 VOI cycle coverage

This cumulative edition includes a disposition for every monthly VOI from January through October 2026. Detailed requirement profiles below carry the operative conclusions; this table prevents an issue with no standalone topic heading from disappearing from the review record.

Issue	Disposition	Durable content carried forward
January 2026	Integrated	SF 312 remote witnessing and acceptance controls; citizenship-evidence limits.
February 2026	Integrated	First-application citizenship verification scope and Rap Back advisements.
March 2026	Integrated	Five-year personnel-vetting update workflow and order-form selection.
April 2026	Integrated in cumulative source digest	Security-in-depth plans for open storage areas; approved equipment procurement; digital signatures for DD 441, SF 312 and SF 328; and DD 254 marking review before NISS upload.
May 2026	Integrated	Five-year PVQ cycle and government-issued CSfC mobile-platform clarification.
June 2026	Integrated	eApp remains the applicant portal after investigation-request work moves to DISS.
July 2026	Integrated	Citizenship verification methods, NISS profile review, and release of ISL 2026-01.
August 2026	Integrated	Rap Back Phase III, CUI training cadence, NAESOC, advertising, check-up, insider-threat, and storage-equipment updates.
September 2026	Integrated	Entity Vetting and ISP routing, administrative findings, Tool 2.0, DCSA credentials, NAESOC, and self-inspection completion.
October 2026	Integrated	NI2 platform announcement, FOCI Expansion for $5M+ contracts, SF-328 updates, agent name changes, FY27 review goal (6,000), FY26 results, Black Label operational restrictions, and NAESOC transitions.

2. Sources and coverage

The catalog includes only approved findings and their recorded Part 117 anchors. Before approval, each topic must pass the concept-and-citation closure gate in the Stage 3 instructions; this deterministic renderer cannot discover an omitted source. Every topic below identifies whether its practice rests on rule text, incorporated authority, or DCSA guidance.

2.1 Authority coverage

• Administrative findings, vulnerabilities, and mitigation follow-up - § 117.7(h)(2); 1 guidance touch(es)

• Advertising positions requiring a Personnel Security Clearance - § 117.9(a)(9); 1 guidance touch(es)

• Changed-condition reporting and Entity Vetting processing - § 117.8(c)(7); 2 guidance touch(es)

• Classified Information Nondisclosure Agreement (SF 312) - § 117.10(g); 3 guidance touch(es)

• CUI training frequency — annual to biennial - § 117.12(f), § 117.18(f); 1 guidance touch(es)

• DCSA representative credentials and classified-visit access - § 117.16(a)(1), § 117.16(a)(3); 2 guidance touch(es)

• Do not search for classified information in the public domain - § 117.15(a), § 117.8(a)(1), § 117.8(d), § 117.18(b)(2); 1 guidance touch(es)

• Fingerprint Collection - § 117.10(e), § 117.10(b)(5); 7 guidance touch(es)

• FY27 security review prioritization and baseline frequency - § 117.7(h); 2 guidance touch(es)

• Information System Security and Commercial Cloud Services - § 117.18; 4 guidance touch(es)

• Insider Threat Program and ITPSO Appointment - § 117.7(b)(4), § 117.7(d), § 117.12(g), § 117.18(a)(1), § 117.18(b)(4); 6 guidance touch(es)

• International plans and notices submission route - § 117.19(d); 1 guidance touch(es)

• MFO classified performance, disclosure, and DD Form 254 locations - § 117.9(i), § 117.13(d), § 117.15(h)(1), § 117.15(h)(3); 7 guidance touch(es)

• NAESOC oversight team verification for newly transitioned facilities - § 117.7(l); 2 guidance touch(es)

• Open Storage Areas (formerly Closed Areas) - § 117.15(c), § 117.15(b); 8 guidance touch(es)

• Reinvestigation and Continuous Vetting - § 117.10(b)(5); 5 guidance touch(es)

• Reporting Requirements and SEAD 3 Reportable Activities - § 117.8, § 117.7(h)(2)(i), § 117.7(h)(2)(ii), § 117.7(h)(2)(iii); 7 guidance touch(es)

• Security Rating Score Tool 2.0 and self-inspection alignment - § 117.7(h)(2); 1 guidance touch(es)

• SF-328 Certificate Pertaining to Foreign Interests — revised form - § 117.11(b), § 117.11(d); 1 guidance touch(es)

• Submission of the SF 86 (NBIS eApp) - § 117.10(d); 6 guidance touch(es)

• Verification of U.S. Citizenship - § 117.10(c); 5 guidance touch(es)

2.2 Changed this cycle (2026-01 and later)

• Administrative findings, vulnerabilities, and mitigation follow-up - catalog correction 2026-09-30: Added the October 2026 split between internal administrative-finding remediation and continuing DCSA validation of vulnerabilities.

• Advertising positions requiring a Personnel Security Clearance - catalog correction 2026-09-01: New topic added from the August 2026 VOI cycle.

• Changed-condition reporting and Entity Vetting processing - catalog correction 2026-09-30: Added the Entity Vetting processing transition while preserving the existing Part 117 reporting duty and NISS submission channel.

• CUI training frequency — annual to biennial - catalog correction 2026-09-01: New topic added from the August 2026 VOI cycle.

• DCSA representative credentials and classified-visit access - catalog correction 2026-10-30: Updated with agent title changes and credential-only standard confirmation.

• Do not search for classified information in the public domain - catalog correction 2026-09-01: New topic added from the August 2026 VOI cycle.

• Fingerprint Collection - catalog correction 2026-09-01: New topic added from the August 2026 VOI cycle.

• FY27 security review prioritization and baseline frequency - catalog correction 2026-10-30: New entry for FY27 review goal, baseline frequency table, and FY26 final results.

• Insider Threat Program and ITPSO Appointment - catalog correction 2026-09-01: New topic added from the August 2026 VOI cycle.

• International plans and notices submission route - catalog correction 2026-09-30: Added the current DCSA routing protocol for international plans and consignment notices.

• MFO classified performance, disclosure, and DD Form 254 locations - catalog correction 2026-08-14: Added the previously omitted MFO chain across Part 117, the DCSA FCL handbook, the November 2023 VOI, the current DD Form 254 instructions, and the current MFO legal-entity boundary job aid.

• NAESOC oversight team verification for newly transitioned facilities - catalog correction 2026-10-30: Updated with account-lockout warning and continued migration status.

• Open Storage Areas (formerly Closed Areas) - catalog correction 2026-10-30: Updated with USW(I&S) operational restrictions and mandatory compliance directives.

• Reporting Requirements and SEAD 3 Reportable Activities - catalog correction 2026-09-01: New topic added from the August 2026 VOI cycle.

• Security Rating Score Tool 2.0 and self-inspection alignment - catalog correction 2026-09-30: Recorded full DCSA implementation and the narrower, recommended status of industry use.

• SF-328 Certificate Pertaining to Foreign Interests — revised form - catalog correction 2026-10-30: New entry for the revised SF-328 form changes and submission triggers.

• Administrative findings, vulnerabilities, and mitigation follow-up - 2026-09-30 VOI September 2026: Effective October 1, 2026, DCSA personnel no longer validate contractor mitigation actions or request formal written mitigation packages for administrative findings; vulnerabilities still require contractor corrective-action responses and DCSA validation.

• Advertising positions requiring a Personnel Security Clearance - 2026-08-31 VOI August 2026: A contractor may advertise employee positions that require a Personnel Security Clearance (PCL) in connection with the position, but may not use its favorable entity eligibility determination (Facility Clearance) for advertising or promotional purposes.

• Changed-condition reporting and Entity Vetting processing - 2026-09-30 VOI September 2026: Effective October 1, 2026, Entity Vetting assumes processing of all cleared-facility changed-condition packages; facilities continue submitting the packages electronically through NISS and the assigned ISR retains completion visibility.

• Changed-condition reporting and Entity Vetting processing - 2026-09-30 VOI September 2026: The Entity Vetting changed-condition processing transition applies to NAESOC facilities; NAESOC no longer processes changed-condition packages after October 1, 2026.

• CUI training frequency — annual to biennial - 2026-08-31 VOI August 2026: Mandatory Controlled Unclassified Information (CUI) training frequency changed from annual to biennial (every two years); CUI training materials and policy are to be updated to match.

• DCSA representative credentials and classified-visit access - 2026-09-30 VOI September 2026: During DCSA's phased credential transition, facilities accept valid CACs and the new DCSA credential for identity, but still verify access authorization in DISS for classified visits and apply the stated limits on retaining, copying, scanning, or using DCSA personnel identity data.

• DCSA representative credentials and classified-visit access - 2026-10-30 VOI October 2026: DCSA is transitioning internal titles: BI Special Agents become Investigators, BI Special Agents in Charge become Supervisory Investigators, and CI Special Agents become CI Specialists. Authorities, responsibilities, and legal frameworks remain unchanged. DCSA has also moved from a badge-and-credentials standard to a credential-only standard; CAC will no longer be used for investigation identification.

• Do not search for classified information in the public domain - 2026-08-31 VOI August 2026: Restates the standing 2017 DCSA (then DSS) notice that NISP contractors should not search for classified information in the public domain.

• Fingerprint Collection - 2026-08-31 VOI August 2026: Industry personnel without fingerprints already on file (Phase III of the Rap Back expansion) must be enrolled in DCSA Rap Back; enrollment in another agency's Rap Back program does not excuse this.

• FY27 security review prioritization and baseline frequency - 2026-10-30 VOI October 2026: DCSA completed 4,526 rated security reviews against a goal of 3,900 (116.1%). Distribution: Superior 564 (12.5%), Commendable 1,717 (37.9%), Satisfactory 2,226 (49.2%), Marginal 6 (0.1%), Unsatisfactory 13 (0.3%).

• FY27 security review prioritization and baseline frequency - 2026-10-30 VOI October 2026: DCSA establishes a goal of 6,000 security reviews for FY27 (up from FY26's 3,900 goal). Publishes a prioritization frequency table: initial review within 12 months of FCL issuance; marginal/unsatisfactory re-review within 12 months; FOCI-mitigated, authorized CIS, and TS-with-storage facilities reviewed annually; Secret/Confidential with storage and FCL-without-storage at least every 3 years. The first applicable row in the table determines baseline frequency.

• Information System Security and Commercial Cloud Services - 2026-05-01 VOI May 2026: Stated that DCSA policy does not prohibit government-issued NSA-approved CSfC mobile platforms at cleared contractor facilities.

• Insider Threat Program and ITPSO Appointment - 2026-07-01 VOI Jul 2026: Current. Announced the formal release of ISL 2026-01, consolidating insider threat minimum standards, resources and training.

• Insider Threat Program and ITPSO Appointment - 2026-08-31 VOI August 2026: DCSA released ISL 2026-01, a consolidated statement of minimum standards, resources, and training for contractor insider threat programs. The VOI states the ISL explicitly incorporates (and by implication supersedes for contractor-facing purposes) guidance previously spread across the Insider Threat Training for Cleared Industry Slick Sheet, the Insider Threat Training Information Paper, and prior VOI Newsletter coverage of the topic.

• International plans and notices submission route - 2026-09-30 VOI September 2026: Effective October 1, 2026, cleared facilities email International Transportation Plans, Hand Carry Plans, and Notices of Consignment directly to the ISP mailbox and courtesy-copy the assigned ISR on every submission and related communication.

• NAESOC oversight team verification for newly transitioned facilities - 2026-08-31 VOI August 2026: Facilities newly assigned to NAESOC oversight should verify in NISS that their assigned oversight team shows “NAESOC” and then direct future inquiries, administrative updates, and safeguarding support to the NAESOC Helpdesk rather than a prior oversight contact.

• NAESOC oversight team verification for newly transitioned facilities - 2026-10-30 VOI October 2026: NAESOC continues welcoming new facilities with rolling migrations. The VOI warns that Government Services Portal accounts inactive for over 30 days are automatically locked and directs users to ServiceNow Helpdesk at 878-274-1003 for regaining access.

• Open Storage Areas (formerly Closed Areas) - 2026-08-31 VOI August 2026: Reiterates the black label GSA container phase-out schedule (authorization to use for classified storage ends per container class/model, October 2024 through October 2028) and that vault doors remain authorized for classified storage until 1 October 2035 per an ISOO extension.

• Open Storage Areas (formerly Closed Areas) - 2026-08-31 VOI August 2026: Sets out the required steps once a black label container reaches end of service: search for and remove all classified material, remove GSA-approval and identification labels, mark the container as no longer GSA approved for continued unclassified filing-cabinet use, or follow the separate disposal procedure (remove/destroy or return limited-use combination locks, and recycle rather than resell) if the container is being disposed of.

• Open Storage Areas (formerly Closed Areas) - 2026-10-30 VOI October 2026: USW(I&S) published administrative guidance on Black Label container phase-out. Authorized uses: internal need-to-know separation within approved open-storage areas and routine combination-lock changes. Explicitly prohibited: primary classified storage outside approved open-storage facilities, and any physical maintenance, structural repair, or locksmith drilling. Mandatory actions: de-label and re-identify with 'No Longer GSA Approved' sticker; replace on mechanical failure with Red Label container; complete retirement from classified operations by October 1, 2028.

• Open Storage Areas (formerly Closed Areas) - 2026-08-31 ISOO Notice 2026-06: Expressly rescinds and replaces ISOO Notices 2022-03 and 2021-01, retains the current black-label equipment deadlines, and consolidates the disposal procedure.

• Reinvestigation and Continuous Vetting - 2026-05-01 VOI May 2026: Current. Periodic reinvestigations are no longer required; submit a PVQ every five years, timed from the DISS PVQ Date.

• Reporting Requirements and SEAD 3 Reportable Activities - 2026-08-31 VOI August 2026: During a facility's FCL anniversary month, DCSA sends the Annual Industry Check-Up Tool as a reminder to check completion of reporting requirements under 32 CFR Part 117 (NISPOM); the tool does not substitute for the required self-inspection.

• Reporting Requirements and SEAD 3 Reportable Activities - 2026-09-30 VOI September 2026: DCSA reminds facilities to ensure the SMO certifies the self-inspection and that completion is annotated in NISS.

• Security Rating Score Tool 2.0 and self-inspection alignment - 2026-09-30 VOI September 2026: Effective October 1, 2026, DCSA field operations use Security Rating Score Tool 2.0 exclusively for post-review calculations and formal facility ratings; facilities are strongly encouraged to use the finalized resources during annual self-inspections.

• SF-328 Certificate Pertaining to Foreign Interests — revised form - 2026-10-30 VOI October 2026: The SF-328 (Certificate Pertaining to Foreign Interests) has been updated since its May 2025 deployment: condensed to nine questions; SEC filings (Schedules 13D/13G) now retrieved by DCSA rather than submitted by the facility; the separate Statement of Full Disclosure of Foreign Affiliations is retired; Question 1 broadened for diverse foreign ownership structures; Question 4 adds 'binding authority' as a means of foreign control; Question 7b foreign-income threshold set at 15%. The form is the standard certificate for FOCI Expansion, CMMC, and SBIR/STTR programs.

• Verification of U.S. Citizenship - 2026-01-01 VOI Jan 2026: Stated that verification must be conducted strictly in person, and identified email, video technology and other remote methods as not authorised.

• Verification of U.S. Citizenship - 2026-01-01 VOI Jan 2026: Listed DISS in a table of documents and systems headed Acceptable Proof for PCL Applicants? against the answer No, stating without qualification that DISS is an internal government database and cannot be used as an official source to validate U.S. citizenship for security clearance applicants.

• Verification of U.S. Citizenship - 2026-01-01 VOI Jan 2026: Provided that where operational needs prevent in-person verification, a trusted third party such as a notary, outside counsel or other government representative may be authorised, subject to written company procedures.

3. Requirements

3.1 § 117.7(h)(2) - Administrative findings, vulnerabilities, and mitigation follow-up

Current-cycle finding: Effective October 1, 2026, DCSA personnel no longer validate contractor mitigation actions or request formal written mitigation packages for administrative findings; vulnerabilities still require contractor corrective-action responses and DCSA validation. Detected or announced in: VOI September 2026 (2026-09-30). Operational basis: 32 CFR 117.7(h)(2); VOI September 2026. The CFR remains controlling.

What DCSA guidance adds to the rule

Beginning October 1, 2026, DCSA no longer validates mitigation or requests formal written mitigation packages for administrative findings. Contractors are still requested to resolve them within 30 days and may use an internal POA&M when resolution takes longer. Vulnerabilities continue to require corrective-action responses and DCSA validation.

Regulatory text - controlling authority

• § 117.7(h)(2) - Procedures (last amended 2024-07-15)

32 CFR 117.7(h)(2) requires continuing program review, an annual formal self-inspection, a report of findings and issue resolution, appropriate corrective actions, and management involvement. DCSA guidance—not the rule text—categorizes non-compliance as an administrative finding, serious vulnerability, or critical vulnerability.

Required practice

#	Basis	Source	Required action
1	Rule [Contractor duty]	32 CFR 117.7(h)(2)	Document self-inspection findings, resolve identified issues, take appropriate corrective actions, and retain the formal report for CSA review.
2	DCSA guidance [Administrative finding]	VOI September 2026	For an administrative finding, resolve the issue without waiting for DCSA mitigation validation or a request for a formal written response; target resolution within 30 calendar days and use an internal POA&M when complexity delays closure.
3	DCSA guidance [Vulnerability]	VOI September 2026	For a vulnerability, provide the contractor corrective-action response and obtain DCSA validation under the continuing process.

Decision paths - which facts point where

Scenario	If	Then
Classify the follow-up path	DCSA identifies a non-compliance after a review or engagement.	1. Confirm whether DCSA categorized it as an administrative finding or a vulnerability. 2. For an administrative finding, document and complete internal remediation; use a POA&M if the 30-day benchmark cannot be met. 3. For a vulnerability, prepare the corrective-action response and support DCSA validation. Do not apply the administrative-finding no-validation process to a vulnerability.

Matters not addressed by the regulation

• Elimination of DCSA validation is limited to administrative findings; it does not eliminate contractor remediation.

• An administrative finding does not automatically become a vulnerability merely because it remains open, but unresolved findings affect later program-effectiveness and Gold Standard evaluation.

Guidance changed in the preceding year

Date	Level	Source	Direction and effect	Status / basis
2026-09-30	VOI	VOI September 2026	Effective October 1, 2026, DCSA personnel no longer validate contractor mitigation actions or request formal written mitigation packages for administrative findings; vulnerabilities still require contractor corrective-action responses and DCSA validation.	active; No supersession conclusion

3.2 § 117.9(a)(9) - Advertising positions requiring a Personnel Security Clearance

Current-cycle finding: A contractor may advertise employee positions that require a Personnel Security Clearance (PCL) in connection with the position, but may not use its favorable entity eligibility determination (Facility Clearance) for advertising or promotional purposes. Detected or announced in: VOI August 2026 (2026-08-31). Operational basis: 32 CFR 117.9(a)(9). The CFR remains controlling.

What DCSA guidance adds to the rule

The VOI clarifies that the same paragraph permits advertising an employee position that itself requires a Personnel Security Clearance; the prohibition is narrowly on using the Facility Clearance itself for advertising/promotional purposes, not on mentioning a PCL requirement in a job posting.

Regulatory text - controlling authority

• § 117.9(a)(9) - Entity eligibility determination for access to classified information (last amended 2024-07-15)

32 CFR Part 117.9(a)(9), as quoted by this source: a contractor will not use its favorable entity eligibility determination (Facility Clearance) for advertising or promotional purposes.

Required practice

#	Basis	Source	Required action
1	Rule [Permitted]	32 CFR 117.9(a)(9)	You may advertise an employee position that requires a Personnel Security Clearance in connection with that position.
2	Rule [Prohibited]	32 CFR 117.9(a)(9)	Do not use the facility's favorable entity eligibility determination (Facility Clearance) itself for advertising or promotional purposes.

Matters not addressed by the regulation

• The permission to mention a PCL requirement in a job posting is not the same as permission to advertise or promote the company using its Facility Clearance status — these are two different clauses of the same paragraph.

Guidance changed in the preceding year

Date	Level	Source	Direction and effect	Status / basis
2026-08-31	VOI	VOI August 2026	A contractor may advertise employee positions that require a Personnel Security Clearance (PCL) in connection with the position, but may not use its favorable entity eligibility determination (Facility Clearance) for advertising or promotional purposes.	active; No supersession conclusion

3.3 § 117.8(c)(7) - Changed-condition reporting and Entity Vetting processing

Current-cycle finding: The Entity Vetting changed-condition processing transition applies to NAESOC facilities; NAESOC no longer processes changed-condition packages after October 1, 2026. Detected or announced in: VOI September 2026 (2026-09-30). Operational basis: 32 CFR 117.8(c)(7); VOI September 2026. The CFR remains controlling.

What DCSA guidance adds to the rule

Effective October 1, 2026, Entity Vetting processes cleared-facility changed-condition packages submitted through NISS. The assigned ISR retains completion visibility but no longer administers the workload. The same route applies to NAESOC facilities, and NAESOC no longer processes these packages.

Regulatory text - controlling authority

• § 117.8(c)(7) - Reporting requirements (last amended 2023-04-05)

32 CFR 117.8(c)(7) requires contractors to report changed conditions affecting entity eligibility, including ownership or control, operating name or address, KMP information, termination or bankruptcy, and material FOCI changes.

Required practice

#	Basis	Source	Required action
1	Rule [Reporting duty]	32 CFR 117.8(c)(7)	Report each covered changed condition affecting entity eligibility promptly and provide the information required by the applicable paragraph.
2	DCSA guidance [Submission route]	VOI September 2026	Submit the changed-condition package electronically through NISS for Entity Vetting processing; do not redirect a NAESOC facility's package to NAESOC.
3	DCSA guidance [Oversight visibility]	VOI September 2026	Treat the assigned ISR as retaining visibility after Entity Vetting completes the package, not as the office administering package review.

Matters not addressed by the regulation

• The October 2026 change reallocates DCSA processing responsibility; it does not narrow the contractor's underlying reporting duty.

• Continue using NISS. The VOI does not replace the electronic package with email submission.

Guidance changed in the preceding year

Date	Level	Source	Direction and effect	Status / basis
2026-09-30	VOI	VOI September 2026	Effective October 1, 2026, Entity Vetting assumes processing of all cleared-facility changed-condition packages; facilities continue submitting the packages electronically through NISS and the assigned ISR retains completion visibility.	active; No supersession conclusion
2026-09-30	VOI	VOI September 2026	The Entity Vetting changed-condition processing transition applies to NAESOC facilities; NAESOC no longer processes changed-condition packages after October 1, 2026.	active; No supersession conclusion

3.4 § 117.10(g) - Classified Information Nondisclosure Agreement (SF 312)

Current operational direction: Where the subject signs in the presence of a witness, the witnessing may be conducted remotely by video. The witness is to be an authorised representative of the contractor or a U.S. executive branch employee; notaries, outside legal counsel and friends or family are identified as not permitted. The FSO or designee signs the acceptance block, by wet or authorised digital signature, before upload. A form uploaded without the acceptance signature is rejected. Source: VOI Jan 2026

(2026-01-30). This is the newest applicable active guidance recorded for this topic; the CFR remains controlling.

What DCSA guidance adds to the rule

The rule requires execution before access, signature in the presence of a witness with matching dates, forwarding to the CSA, and a report on refusal. Guidance modifies the witnessing requirement and supplies the mechanics: ECA PKI digital signatures are accepted; no witness signature is required where the subject signs digitally; witnessing may be conducted remotely by video; the permitted witness population is defined and narrowed; the FSO signs an acceptance block; and retention is by upload to DISS, which the rule does not name.

Regulatory text - controlling authority

• § 117.10(g) - Determination of eligibility for access to classified information for contractor employees (last amended 2021-02-26)

An employee determined eligible for access must execute the NDA before being granted access. The employee must sign and date the NDA in the presence of a witness, and the two signatures must bear the same date. The contractor forwards the executed NDA to the CSA for retention. If the employee refuses to execute it, deny access and report under §117.8(c)(6).

Required practice

#	Basis	Source	Required action
1	Rule	32 CFR 117.10(g)(1)	The NDA is executed before access is granted.
2	DCSA guidance	VOI Jan 2025	A digital signature using a DoD Sponsored or Approved ECA PKI certificate is accepted. Wet signatures remain acceptable.
3	DCSA guidance	VOI Jan 2025	Where the subject signs using an authorised digital signature, a witness signature is not required.
4	DCSA guidance	VOI Jan 2026	Where the subject signs in the presence of a witness, the witnessing may be conducted remotely by video. The witness is to be an authorised representative of the contractor or a U.S. executive branch employee; notaries, outside legal counsel and friends or family are identified as not permitted.
5	DCSA guidance	VOI Jan 2026	The FSO or designee signs the acceptance block, by wet or authorised digital signature, before upload. A form uploaded without the acceptance signature is rejected.
6	DCSA guidance	VOI Mar 2025	Upload the fully executed NDA to the subject's DISS record. A new agreement is not required where an NDA Signed Date already appears in JVS and no pending SF 312 notification is present.
7	Rule	32 CFR 117.10(g)(3)	Forward the executed NDA to the CSA for retention. The CSA may authorize the contractor to retain a copy for administrative purposes where appropriate — retention by the contractor is permitted, not assumed.
8	Rule	32 CFR 117.10(g)(4)	Where the employee refuses to execute the NDA, deny access and submit a report under §117.8(c)(6).

Matters not addressed by the regulation

• The witness provision in the rule is stated without qualification. §117.10(g)(2) provides that the employee signs in the presence of a witness with matching dates. The January 2025 guidance provides that a witness signature is not required where the subject uses an authorised digital signature. Read narrowly, that applies to that signature method and is not extended further here.

• Remote witnessing is addressed in guidance rather than in the rule. The January 2026 article provides for video witnessing where a witness is used.

• The permitted witness population is narrower than may be assumed. Notaries and outside legal counsel are identified as not permitted for this purpose, although notaries are permitted elsewhere in DCSA guidance for other functions.

• The rule does not name a system for retention. It provides that the executed NDA is forwarded to the CSA; DCSA guidance directs upload into DISS.

Guidance changed in the preceding year

Date	Level	Source	Direction and effect	Status / basis
2022-05-01	VOI	VOI May 2022	Provided that notwithstanding ISOO Notice 2022-01 addressing digital signatures, contractors under DoD cognizance were to continue having employees physically sign the SF 312 pending DoD or DCSA guidance.	superseded; INFERRED - Superseded by the January 2025 guidance authorising ECA PKI digital signatures. Procedures adopted on the 2022 basis are worth revisiting.
2026-01-30	VOI	VOI Jan 2026	Where the subject signs in the presence of a witness, the witnessing may be conducted remotely by video. The witness is to be an authorised representative of the contractor or a U.S. executive branch employee; notaries, outside legal counsel and friends or family are identified as not permitted. The FSO or designee signs the acceptance block, by wet or authorised digital signature, before upload. A form uploaded without the acceptance signature is rejected.	active; No supersession conclusion

Reviewer note: The January 2026 issue records a DISS defect that caused rejection of digitally signed SF 312s and directs resubmission of previously rejected forms for subjects still affiliated with the entity. For separated subjects it directs contacting the Customer Engagements Team with the name, CAGE code and last day of employment rather than resubmitting.

3.5 § 117.12(f), § 117.18(f) - CUI training frequency — annual to biennial

Current-cycle finding: Mandatory Controlled Unclassified Information (CUI) training frequency changed from annual to biennial (every two years); CUI training materials and policy are to be updated to match. Detected or announced in: VOI August 2026 (2026-08-31). Operational basis: 32 CFR 117.12(f) and 117.18(f); VOI August 2026; DoDI 5200.48 / DCSA Training Template Version 3. The CFR remains controlling.

What DCSA guidance adds to the rule

The August 2026 VOI announces a biennial training cadence. Current DoDI 5200.48 and DCSA Training Template Version 3 still state annual training, so the sources presently conflict and the contract-specific requirement must be preserved until the controlling issuances are reconciled.

Regulatory text - controlling authority

Part 117 states that controlled unclassified information is outside the NISPOM unless protection is required by the contract or another applicable authority. The contract and the controlling CUI issuance therefore govern the required training cadence.

Required practice

#	Basis	Source	Required action
1	Rule	32 CFR 117.12(f) and 117.18(f)	Apply the contract and controlling CUI authority because Part 117 does not itself establish the CUI training cadence.
2	DCSA guidance	VOI August 2026	Record DCSA's announced change from annual to biennial CUI training.
3	DCSA guidance	DoDI 5200.48 / DCSA Training Template Version 3	Where the contract or controlling issuance still requires annual training, continue the annual cadence until an authoritative revision resolves the conflict.

Matters not addressed by the regulation

• No effective date is given for when updated CUI training materials/policy will actually be published — do not assume the biennial cycle is already reflected in current course offerings.

Guidance changed in the preceding year

Date	Level	Source	Direction and effect	Status / basis
2026-08-31	VOI	VOI August 2026	Mandatory Controlled Unclassified Information (CUI) training frequency changed from annual to biennial (every two years); CUI training materials and policy are to be updated to match.	active; No supersession conclusion

Reviewer note: CONFLICT: The August 2026 VOI says biennial CUI training, while the currently published DoDI 5200.48 and DCSA Training Template Version 3 say annual. Do not relax a contractual or controlling annual requirement on the VOI announcement alone.

3.6 § 117.16(a)(1), § 117.16(a)(3) - DCSA representative credentials and classified-visit access

Current-cycle finding: DCSA is transitioning internal titles: BI Special Agents become Investigators, BI Special Agents in Charge become Supervisory Investigators, and CI Special Agents become CI Specialists. Authorities, responsibilities, and legal frameworks remain unchanged. DCSA has also moved from a badge-and-credentials standard to a credential-only standard; CAC will no longer be used for investigation identification. Detected or announced in: VOI October 2026 (2026-10-30). Operational basis: 32 CFR 117.16(a)(1), (3); VOI September 2026. The CFR remains controlling.

What DCSA guidance adds to the rule

Beginning October 1, 2026, DCSA oversight personnel transition from CACs to DCSA credentials. During the transition, facilities accept either valid credential for identity, but verify classified access separately through DISS. The VOI also limits local retention, copying, scanning, PII storage, servicing relationships, and added local agreements for DCSA personnel. In October 2026, DCSA announced title changes: BI Special Agents are now Investigators, BI SACs are Supervisory Investigators, and CI Special Agents are CI Specialists. The move to credential-only (no CAC for investigation identification) is confirmed.

Regulatory text - controlling authority

• § 117.16(a)(1) - Visits and meetings (last amended 2021-02-26)

• § 117.16(a)(3) - Visits and meetings (last amended 2021-02-26)

32 CFR 117.16(a) requires positive visitor identification, appropriate PCL and need-to-know before classified disclosure, limits access to the visit purpose, and permits official USG inspectors, investigators, and auditors to visit when they present appropriate USG credentials.

Required practice

#	Basis	Source	Required action
1	Rule [Visit baseline]	32 CFR 117.16(a)(1), (3)	Positively identify the visiting government representative and independently satisfy the classified-visit access, need-to-know, and purpose controls before disclosure.
2	DCSA guidance [Identity]	VOI September 2026	During the phased transition, visually inspect and accept either a valid CAC or DCSA credential as identity evidence; do not treat the physical credential as clearance verification.
3	DCSA guidance [Access verification]	VOI September 2026	Verify access authorization in DISS by one-time lookup or VAR for a classified visit, provide required program-specific briefings, and do not establish a DISS servicing relationship with DCSA personnel.
4	DCSA guidance [Local controls]	VOI September 2026	Do not retain, scan, swipe, or photocopy the credential; store DCSA personnel PII in an unapproved database; share it with third parties; or require additional local agreements, waivers, or NDAs for DCSA oversight work.

Matters not addressed by the regulation

• A CAC or DCSA credential confirms identity, not eligibility, access authorization, need-to-know, or visit purpose.

• The transition is phased; a facility must not reject an otherwise valid CAC merely because DCSA credentials have begun issuing.

Guidance changed in the preceding year

Date	Level	Source	Direction and effect	Status / basis
2026-09-30	VOI	VOI September 2026	During DCSA's phased credential transition, facilities accept valid CACs and the new DCSA credential for identity, but still verify access authorization in DISS for classified visits and apply the stated limits on retaining, copying, scanning, or using DCSA personnel identity data.	active; No supersession conclusion
2026-10-30	VOI	VOI October 2026	DCSA is transitioning internal titles: BI Special Agents become Investigators, BI Special Agents in Charge become Supervisory Investigators, and CI Special Agents become CI Specialists. Authorities, responsibilities, and legal frameworks remain unchanged. DCSA has also moved from a badge-and-credentials standard to a credential-only standard; CAC will no longer be used for investigation identification.	active; No supersession conclusion

Reviewer note: DCSA Background Investigation personnel transition later in calendar year 2026; later VOIs may refine that timetable.

3.7 § 117.15(a), § 117.8(a)(1), § 117.8(d), § 117.18(b)(2) - Do not search for classified information in the public domain

Current-cycle finding: Restates the standing 2017 DCSA (then DSS) notice that NISP contractors should not search for classified information in the public domain. Detected or announced in: VOI August 2026 (2026-08-31). Operational basis: 2017 DCSA (then DSS) Notice to Contractors Cleared Under the NISP on Inadvertent Exposure to Classified in the Public Domain (as restated in VOI August 2026). The CFR remains controlling.

What DCSA guidance adds to the rule

The August 2026 VOI repeats the June 2017 DCSA direction not to search for classified information in the public domain. If inadvertent exposure creates a suspected compromise or spill, the applicable Part 117 inquiry and reporting duties still govern.

Regulatory text - controlling authority

Part 117 requires safeguarding classified information and reporting or investigating loss, compromise, suspected compromise, and data spills. It does not direct contractor personnel to seek out classified material in public sources.

Required practice

#	Basis	Source	Required action
1	DCSA guidance [Standing reminder]	2017 DCSA (then DSS) Notice to Contractors Cleared Under the NISP on Inadvertent Exposure to Classified in the Public Domain (as restated in VOI August 2026)	Do not search for classified information in the public domain.

Guidance changed in the preceding year

Date	Level	Source	Direction and effect	Status / basis
2026-08-31	VOI	VOI August 2026	Restates the standing 2017 DCSA (then DSS) notice that NISP contractors should not search for classified information in the public domain.	active; No supersession conclusion

Reviewer note: The 2017 notice itself is not in this corpus; this entry rests entirely on the VOI's restatement of it.

3.8 § 117.10(e), § 117.10(b)(5) - Fingerprint Collection

Current-cycle finding: Industry personnel without fingerprints already on file (Phase III of the Rap Back expansion) must be enrolled in DCSA Rap Back; enrollment in another agency's Rap Back program does not excuse this. Detected or announced in: VOI August 2026 (2026-08-31). Operational basis: VOI Jul 2025; VOI Nov 2023; VOI Nov 2018; VOI Feb 2020; VOI Feb 2026; 32 CFR 117.10(e); VOI August 2026. The CFR remains controlling.

What DCSA guidance adds to the rule

The rule is two sentences: submit in accordance with CSA guidance, use digital fingerprints where possible. It contains no operational content at all. Submission timing, the 120-day validity window, the SWFT ALC code, the prohibition on requesting prints for reinvestigations, and the Rap Back advisement duty are all supplied by guidance. This is the widest rule-to-guidance gap in the document. The August 2026 VOI confirms the phased Rap Back expansion has reached Phase III (industry personnel without fingerprints already on file) and states enrollment in another agency's Rap Back program does not excuse DCSA enrollment when an individual appears on a Phase III list.

Regulatory text - controlling authority

• § 117.10(e) - Determination of eligibility for access to classified information for contractor employees (last amended 2021-02-26)

The contractor will submit fingerprints in accordance with CSA guidance. Contractors will use digital fingerprints whenever possible. That is the entire rule text. Every operational detail below exists only in guidance.

Required practice

#	Basis	Source	Required action
1	DCSA guidance	VOI Jul 2025	Submit electronic fingerprints at the same time the investigation request is sent to the subject for completion.
2	DCSA guidance	VOI Nov 2023	Fingerprint results are valid 120 days, the same period for which eApp signature pages are valid.
3	DCSA guidance	VOI Nov 2018	Reinvestigation submissions should not request fingerprints. Where FIPC Code I is added, the system holds the fingerprint request for 14 days and then rejects the case.
4	DCSA guidance	VOI Feb 2020	Use ALC code 97008801 for SWFT submissions; the legacy DSS-IND code is rejected.
5	DCSA guidance	VOI Feb 2026	As FBI Rap Back enrolment expands, distribute the mandatory FBI advisements to cleared employees and incorporate them into onboarding.
6	Rule	32 CFR 117.10(e)	Submit fingerprints in accordance with CSA guidance, using digital fingerprints wherever possible.
7	DCSA guidance [Enrollment]	VOI August 2026	If your facility received a Phase III list of personnel without fingerprints on file, ensure every listed individual is enrolled in DCSA Rap Back, even if they are already enrolled in another agency's Rap Back program.

Matters not addressed by the regulation

• §117.10(e) consists of two sentences. Timing, the validity window, ALC codes and the reinvestigation exception are all set by guidance rather than by the rule, so the rule text alone provides little operational direction.

• The timing instruction was revised in July 2025. From 2016 through January 2025 DCSA directed submission at the same time as, or just before, release of the request to DCSA. The current instruction is to submit when the request is sent to the subject, which falls earlier in the workflow. Procedures written before July 2025 will reflect the earlier instruction.

• Requesting fingerprints on a reinvestigation has a consequence. Rather than being disregarded, the request causes the case to be rejected after 14 days.

• Not every SMO received a Phase III list — only those with ownership of individuals lacking fingerprints on file. Absence of a list does not by itself confirm full enrollment.

Guidance changed in the preceding year

Date	Level	Source	Direction and effect	Status / basis
2025-01-01	VOI	VOI Jan 2025	Submit at the same time as or just before the request is released to DCSA in DISS.	superseded; INFERRED - The last restatement of the old rule, six months before reversal.
2025-07-01	VOI	VOI Jul 2025	Current. Submit prints when the request is sent to the subject for completion.	active; No supersession conclusion
2026-02-27	VOI	VOI Feb 2026	As FBI Rap Back enrolment expands, distribute the mandatory FBI advisements to cleared employees and incorporate them into onboarding.	active; No supersession conclusion
2026-08-31	VOI	VOI August 2026	Industry personnel without fingerprints already on file (Phase III of the Rap Back expansion) must be enrolled in DCSA Rap Back; enrollment in another agency's Rap Back program does not excuse this.	active; No supersession conclusion

Reviewer note: The earlier timing instruction was in place for an extended period and was restated in substantially the same terms across many issues. Procedures drafted before July 2025 are worth checking against that issue specifically.

3.9 § 117.7(h) - FY27 security review prioritization and baseline frequency

Current-cycle finding: DCSA establishes a goal of 6,000 security reviews for FY27 (up from FY26's 3,900 goal). Publishes a prioritization frequency table: initial review within 12 months of FCL issuance; marginal/unsatisfactory re-review within 12 months; FOCI-mitigated, authorized CIS, and TS-with-storage facilities reviewed annually; Secret/Confidential with storage and FCL-without-storage at least every 3 years. The first applicable row in the table determines baseline frequency. Detected or announced in: VOI October 2026 (2026-10-30). Operational basis: VOI October 2026; NISPOM (32 CFR Part 117). The CFR remains controlling.

What DCSA guidance adds to the rule

DCSA sets an FY27 goal of 6,000 security reviews, up from FY26's 3,900 goal. The baseline frequency table (first applicable row determines frequency): initial reviews within 12 months of FCL; marginal/unsatisfactory re-reviews within 12 months; FOCI-mitigated, authorized CIS, and TS-with-storage annually; Secret/Confidential with storage and FCL-without-storage at least every 3 years. FY26 final results: 4,526 completed (116.1% of goal), with 0.4% marginal/unsatisfactory combined.

Regulatory text - controlling authority

• § 117.7(h) - Procedures (last amended 2024-07-15)

32 CFR 117.7(h) authorizes DCSA to conduct security reviews of cleared contractor facilities. The NISPOM requires facilities to maintain continuous readiness including self-inspection.

Required practice

#	Basis	Source	Required action
1	DCSA guidance [Self-assessment]	VOI October 2026	Identify your facility's row in the baseline frequency table to anticipate when your next review is likely. Maintain continuous self-inspection and readiness.
2	Rule [Readiness]	NISPOM (32 CFR Part 117)	Ensure the SMO certifies the self-inspection and annotates completion in NISS before the scheduled review.

Matters not addressed by the regulation

• The frequency table is a baseline; DCSA may adjust scheduling based on emerging risk indicators.

• The 6,000 goal represents a 54% increase over FY26's 3,900 goal; the probability of being reviewed in FY27 is higher.

Guidance changed in the preceding year

Date	Level	Source	Direction and effect	Status / basis
2026-10-30	VOI	VOI October 2026	DCSA completed 4,526 rated security reviews against a goal of 3,900 (116.1%). Distribution: Superior 564 (12.5%), Commendable 1,717 (37.9%), Satisfactory 2,226 (49.2%), Marginal 6 (0.1%), Unsatisfactory 13 (0.3%).	active; No supersession conclusion
2026-10-30	VOI	VOI October 2026	DCSA establishes a goal of 6,000 security reviews for FY27 (up from FY26's 3,900 goal). Publishes a prioritization frequency table: initial review within 12 months of FCL issuance; marginal/unsatisfactory re-review within 12 months; FOCI-mitigated, authorized CIS, and TS-with-storage facilities reviewed annually; Secret/Confidential with storage and FCL-without-storage at least every 3 years. The first applicable row in the table determines baseline frequency.	active; No supersession conclusion

Reviewer note: Actual scheduling may differ from baseline. A marginal or unsatisfactory rating triggers a compliance review within 12 months.

3.10 § 117.18 - Information System Security and Commercial Cloud Services

Current-cycle finding: Stated that DCSA policy does not prohibit government-issued NSA-approved CSfC mobile platforms at cleared contractor facilities. Detected or announced in: VOI May 2026 (2026-05-01). Operational basis: 32 CFR 117.18(b); 32 CFR 117.18(c)(2); 32 CFR 117.18(c)(2)(iv); VOI Dec 2025; 32 CFR 117.18(e)(6); ISL 2024-01; VOI Sep 2025; VOI May 2026. The CFR remains controlling.

What DCSA guidance adds to the rule

The rule requires a risk-based information system security program in accordance with CSA-provided guidance and never says which document that is. Two things fill the gap: ISL 2024-01 supplies the three methods by which DCSA verifies a contract requirement for IL6 commercial cloud services, which the rule does not mention at all; and the DCSA Assessment and Authorization Guide (DAAG) replaced the DAAPM on 1 October 2025. Guidance also settles how the self-inspection interval is read — every 12 months for classified systems, without the calendar-year flexibility applied elsewhere.

Regulatory text - controlling authority

• § 117.18 - Information system security (last amended 2023-04-05)

Contractor information systems that capture, create, store, process or distribute classified information must be protected against unauthorized disclosure using a risk-based approach in accordance with CSA-provided guidance. The contractor maintains an information system security program covering policies and procedures across the system life cycle; plans to assess, report, isolate and contain data spills including sanitization and recovery; security training; insider threat components including user activity monitoring; continual evaluation of threats and vulnerabilities; change control identifying security-relevant changes that may require re-authorization; and banners and user agreements. Contractors processing classified information appoint an employee ISSM. The CSA must authorize the system before it is used to process classified information.

Required practice

#	Basis	Source	Required action
1	Rule	32 CFR 117.18(b)	Maintain an information system security program covering the seven listed components, including data spill assess, report, isolate and contain procedures with sanitization and recovery methods, change control for security-relevant changes, and banners and user agreements.
2	Rule	32 CFR 117.18(c)(2)	Appoint an employee ISSM, adequately trained and technically competent for the complexity of the system, who certifies in writing to the CSA that the systems security plan is implemented for each authorized system.
3	Rule	32 CFR 117.18(c)(2)(iv)	The ISSM verifies self-inspections at least every 12 months on classified information systems, and that corrective action is taken for all identified findings.
4	DCSA guidance	VOI Dec 2025	For facilities with classified systems the 12-month interval is literal — the “calendar year” flexibility does not apply.
5	Rule	32 CFR 117.18(e)(6)	The CSA must authorize the system before the contractor uses it to process classified information.
6	Binding DCSA supplementary procedures	ISL 2024-01	To use IL6 commercial cloud services on a classified contract, DCSA must be able to verify the contract requirement by one of three methods: DD Form 254 block 11c checked with IL6 CCS detail in item 13; verification to DCSA that DFARS clause 252.239-7010 is in each applicable contract; or proof of contracting officer approval — which may be an email — where CCS use was decided after solicitation.
7	Binding DCSA supplementary procedures	ISL 2024-01	Where DFARS 252.239-7010 is in the contract, comply with the DISA Cloud Computing Security Requirements Guide. DCSA determines whether the proposed service meets DISA provisional authorization requirements.
8	DCSA guidance	VOI Sep 2025	Use the DCSA Assessment and Authorization Guide (DAAG) for all RMF authorization work from 1 October 2025. It supersedes all versions of the DAAPM. Download it from NISP eMASS or request it from NCSO.
9	DCSA guidance	VOI Sep 2025	A customer risk acceptance memo is not required to move an unclassified vendor activation code off a classified system using the DCSA-approved AFT process with ASCII text verification, provided the AFT procedures are authorised in your ATO.

#	Basis	Source	Required action
10	DCSA guidance	VOI May 2026	Government-issued NSA-approved CSfC classified tablets, phones and laptops are not prohibited at cleared contractor facilities. The former prohibition addressed legacy flyaway kits, and DCSA has no cognizant security authority over these devices.

Matters not addressed by the regulation

• The rule points at guidance it does not name. §117.18(a)(1) and (b) both require compliance “in accordance with CSA-provided guidance”. Which document that is has changed — the DAAPM until 1 October 2025, the DAAG since.

• Commercial cloud appears nowhere in the rule. The three IL6 verification methods exist only in ISL 2024-01.

• §117.18(b) was the most-cited FY25 deficiency, but it applied to only 13.5% of NISP facilities — those with current or pending authorized systems. The citation rate reflects concentration, not universality.

• The CSfC position reversed. A procedure treating all classified mobile devices as prohibited at the facility reflects guidance the May 2026 issue withdrew.

Guidance changed in the preceding year

Date	Level	Source	Direction and effect	Status / basis
2024-01-01	ISL	ISL 2024-01	Set out the three methods by which DCSA verifies a contract requirement for IL6 commercial cloud services.	active; No supersession conclusion
2025-09-01	VOI	VOI Sep 2025	Announced the DCSA Assessment and Authorization Guide (DAAG), effective 1 October 2025, stating that it supersedes all versions of the DAAPM.	active; No supersession conclusion
2025-12	VOI	VOI Dec 2025	For facilities with classified systems the 12-month interval is literal — the “calendar year” flexibility does not apply.	active; No supersession conclusion
2026-05-01	VOI	VOI May 2026	Stated that DCSA policy does not prohibit government-issued NSA-approved CSfC mobile platforms at cleared contractor facilities.	active; No supersession conclusion

Reviewer note: §117.18(b) is the most-cited deficiency in DCSA's FY25 security reviews. The May 2026 issue names the recurring gaps: RMF control implementation, life-cycle risk policies, data spill assess/report/isolate/contain and sanitization plans, security training, banners and user agreements, insider threat monitoring policies, and change control for security-relevant changes requiring re-authorization. If you hold an authorized system, that list is the self-inspection agenda.

3.11 § 117.7(b)(4), § 117.7(d), § 117.12(g), § 117.18(a)(1), § 117.18(b)(4) - Insider Threat Program and ITPSO Appointment

Current-cycle finding: DCSA released ISL 2026-01, a consolidated statement of minimum standards, resources, and training for contractor insider threat programs. The VOI states the ISL explicitly incorporates (and by implication supersedes for contractor-facing purposes) guidance previously spread across the Insider Threat Training for Cleared Industry Slick Sheet, the Insider Threat Training Information Paper, and prior VOI Newsletter coverage of the topic. Detected or announced in: VOI August 2026 (2026-08-31). Operational basis: 32 CFR 117.7(b)(4); ISL 2026-01; 32 CFR 117.12(g)(1)-(2); ISL 2026-01 (as announced in VOI August 2026). The CFR remains controlling.

What DCSA guidance adds to the rule

The rule requires an insider threat program and an ITPSO, and places training obligations at §117.12(g). It does not say how the appointment is made or evidenced. ISL 2026-01 supplies the mechanism: appointment on the KMP list in NISS with separate letters optional; the FSO as an integral member where not serving as ITPSO; separate appointment at each entity where a family shares one ITPSO, plus an implementation plan to DCSA; the specific training courses and the 1 July 2025 exemption cutoff; and inclusion of insider threat compliance in the annual self-inspection. ISL 2026-01 consolidates minimum standards, resources, and training for contractor insider threat programs into one document, replacing the need to separately consult the Insider Threat Training for Cleared Industry Slick Sheet, the Insider Threat Training Information Paper, and scattered prior VOI Newsletter coverage.

Regulatory text - controlling authority

• § 117.7(b)(4) - Procedures (last amended 2024-07-15)

Contractors must establish and maintain an insider threat program to gather, integrate and report relevant information indicating a potential or actual insider threat, and must designate an Insider Threat Program Senior Official. Training obligations sit at §117.12(g). The rule states the obligation; it does not tell you how DCSA expects it to be evidenced.

Required practice

#	Basis	Source	Required action
1	Rule	32 CFR 117.7(b)(4)	Establish and maintain an insider threat program, and designate an ITPSO.
2	Binding DCSA supplementary procedures	ISL 2026-01	Create and maintain written procedures for the program. CDSE publishes a sample plan for reference.
3	Binding DCSA supplementary procedures	ISL 2026-01	Appoint a U.S. citizen employee in writing as ITPSO on the Key Management Personnel list in NISS. Separate appointment letters are optional. The ITPSO must have authority to manage the program and hold a clearance at the level of the facility clearance.
4	Binding DCSA supplementary procedures	ISL 2026-01	The FSO may serve as the ITPSO. If not, the FSO must be an integral member of the insider threat program team.
5	Binding DCSA supplementary procedures	ISL 2026-01	For an entity family using one ITPSO, each cleared entity must separately appoint that person on its own KMP list in NISS, and the ITPSO must give DCSA an implementation plan for executing the program across the family.
6	Binding DCSA supplementary procedures	ISL 2026-01	The ITPSO and other program personnel must complete one-time specialized training — INT 333.CU, or a contractor-developed programme covering the §117.12(g) topics. The ITPSO is responsible for identifying all program personnel at the facility.
7	Rule	32 CFR 117.12(g)(1)-(2)	All cleared employees receive insider threat awareness training before being granted access, and annually thereafter.
8	Binding DCSA supplementary procedures	ISL 2026-01	Include insider threat program compliance in your annual self-inspection. DCSA assesses against it.
9	Binding DCSA supplementary procedures	ISL 2026-01	Retain training proof keyed to the 1 July 2025 cutoff: ITPSOs appointed before that date need proof of completing INT122.16 or an equivalent contractor programme; ITPSOs reappointed after it need proof of having completed INT122.16 prior to 1 July 2025.
10	Binding DCSA supplementary procedures [Current reference]	ISL 2026-01 (as announced in VOI August 2026)	Use ISL 2026-01 as the current consolidated reference for establishing or tailoring a facility insider threat program, rather than the older Slick Sheet, Information Paper, or scattered VOI coverage.

Matters not addressed by the regulation

• Appointment is made on the KMP list in NISS. ISL 2026-01 provides that the ITPSO is appointed in writing on the KMP list in NISS and that separate appointment letters are optional. Where a facility relies on an appointment letter, it is worth confirming the NISS entry is also in place.

• An entity family-wide ITPSO is appointed at each entity. Each cleared entity using the entity-wide ITPSO appoints that person separately on its own KMP list, and the ITPSO provides DCSA an implementation plan for the entity family.

• Insider threat compliance is to be included in the annual self-inspection. This is stated in ISL 2026-01 rather than in the rule.

• The 1 July 2025 date operates differently for appointments and reappointments. ITPSOs appointed before that date retain proof of the previous training or an equivalent contractor programme; ITPSOs reappointed after that date retain proof of having completed that training prior to 1 July 2025.

• Identifying program personnel is an ITPSO responsibility. The specialised training requirement extends to individuals managing the program, and ISL 2026-01 assigns the ITPSO responsibility for identifying them.

• The VOI's own language ("incorporates guidance previously provided in") is evidence of consolidation, not a verbatim withdrawal quote from the Slick Sheet or Information Paper themselves — treat the relationship as EXPLICIT only once ISL 2026-01's own text is read and, ideally, the two prior documents are checked for their own withdrawal language.

Guidance changed in the preceding year

Date	Level	Source	Direction and effect	Status / basis
2024-12-01	VOI	VOI Dec 2024	Dropped the Insider Threat Detection Analysis Course prerequisites (INT311.CU and INT312.CU) effective immediately.	superseded; INFERRED - Overtaken by the ISL 2026-01 training table, which sets INT 333.CU as the program-personnel path.
2025-04-01	VOI	VOI Apr 2025	Stated that insider threat training designations were under review.	superseded; INFERRED - Resolved by ISL 2026-01.

Date	Level	Source	Direction and effect	Status / basis
2026-05-20	ISL	ISL 2026-01	Create and maintain written procedures for the program. CDSE publishes a sample plan for reference. Appoint a U.S. citizen employee in writing as ITPSO on the Key Management Personnel list in NISS. Separate appointment letters are optional. The ITPSO must have authority to manage the program and hold a clearance at the level of the facility clearance. The FSO may serve as the ITPSO. If not, the FSO must be an integral member of the insider threat program team. For an entity family using one ITPSO, each cleared entity must separately appoint that person on its own KMP list in NISS, and the ITPSO must give DCSA an implementation plan for executing the program across the family. The ITPSO and other program personnel must complete one-time specialized training — INT 333.CU, or a contractor-developed programme covering the §117.12(g) topics. The ITPSO is responsible for identifying all program personnel at the facility. Include insider threat program compliance in your annual self-inspection. DCSA assesses against it. Retain training proof keyed to the 1 July 2025 cutoff: ITPSOs appointed before that date need proof of completing INT122.16 or an equivalent contractor programme; ITPSOs reappointed after it need proof of having completed INT122.16 prior to 1 July 2025.	active; No supersession conclusion
2026-07-01	VOI	VOI Jul 2026	Current. Announced the formal release of ISL 2026-01, consolidating insider threat minimum standards, resources and training.	active; No supersession conclusion
2026-08-31	VOI	VOI August 2026	DCSA released ISL 2026-01, a consolidated statement of minimum standards, resources, and training for contractor insider threat programs. The VOI states the ISL explicitly incorporates (and by implication supersedes for contractor-facing purposes) guidance previously spread across the Insider Threat Training for Cleared Industry Slick Sheet, the Insider Threat Training Information Paper, and prior VOI Newsletter coverage of the topic.	active; No supersession conclusion

Reviewer note: ISL 2026-01 is dated 20 May 2026 and was announced in the July 2026 Voice of Industry. It is one of the four Industrial Security Letters DCSA currently publishes. Because it consolidates material previously carried across a slick sheet, an information paper and several newsletters, an insider threat procedure written before mid-2026 is worth reviewing against it, particularly the ITPSO appointment mechanics.

3.12 § 117.19(d) - International plans and notices submission route

Current-cycle finding: Effective October 1, 2026, cleared facilities email International Transportation Plans, Hand Carry Plans, and Notices of Consignment directly to the ISP mailbox and courtesy-copy the assigned ISR on every submission and related communication. Detected or announced in: VOI September 2026 (2026-09-30). Operational basis: 32 CFR 117.19(d); VOI September 2026. The CFR remains controlling.

What DCSA guidance adds to the rule

Effective October 1, 2026, ISP is the DCSA processing office for International Transportation Plans, Hand Carry Plans, and Notices of Consignment. Industry emails these submissions to the ISP inquiries mailbox and always courtesy-copies the assigned ISR.

Regulatory text - controlling authority

• § 117.19(d) - International security requirements (last amended 2024-07-15)

32 CFR 117.19(d) governs international transfers of classified material, including written transmission instructions, transportation plans, notices for repetitive consignments, and authorization of international hand carrying.

Required practice

#	Basis	Source	Required action
1	Rule [Substantive requirement]	32 CFR 117.19(d)	Prepare and coordinate the applicable written international-transfer, transportation-plan, consignment, or hand-carry documentation required for the transaction.
2	DCSA guidance [DCSA submission route]	VOI September 2026	Email International Transportation Plans, Hand Carry Plans, and Notices of Consignment to dcsa.iob@mail.mil and courtesy-copy the assigned ISR on the submission and related correspondence.

Matters not addressed by the regulation

• The mailbox direction changes DCSA workflow ownership; it does not replace the approvals, government coordination, DGR, export, escort, receipt, or safeguarding requirements in §117.19(d).

• Sending only to the ISR is not the current route; an ISR who receives it alone will forward it to ISP.

Guidance changed in the preceding year

Date	Level	Source	Direction and effect	Status / basis
2026-09-30	VOI	VOI September 2026	Effective October 1, 2026, cleared facilities email International Transportation Plans, Hand Carry Plans, and Notices of Consignment directly to the ISP mailbox and courtesy-copy the assigned ISR on every submission and related communication.	active; No supersession conclusion

3.13 § 117.9(i), § 117.13(d), § 117.15(h)(1), § 117.15(h)(3) - MFO classified performance, disclosure, and DD Form 254 locations

Current operational direction: DCSA states that a parent-subsidiary relationship is not an MFO because the parent and subsidiary are separate legal entities executing separate DD Forms 441. Source: DCSA SMO Slick Sheet, Version 2.0 (2025-11-01). This is the newest applicable active guidance recorded for this topic; the CFR remains controlling.

What DCSA guidance adds to the rule

DCSA's handbook and current SMO job aid define the MFO boundary as one legal entity whose cleared branches and divisions are carried on DD Form 441-1. The November 2023 VOI adds that a cleared MFO performance location omitted from a DD Form 254 does not necessarily require a DD Form 254 update. The current DD Form 254 instructions, updated July 11, 2025, require Item 8 to list every location where the contract defines classified performance and specifically require Item 8 completion for Item 11c performance at divisions or branches. Read together and narrowly: clearance alone does not automatically trigger a revision, but the VOI does not erase the contract, Item 8, eligibility, safeguarding, need-to-know, or classification-guidance requirements. The most recent applicable instruction controls within its scope; unresolved location ambiguity goes to the ISR, Field Office Chief, and GCA rather than being treated as blanket MFO permission.

Regulatory text - controlling authority

• § 117.9(i) - Entity eligibility determination for access to classified information (last amended 2024-07-15)

• § 117.13(d) - Classification (last amended 2024-07-15)

• § 117.15(h)(1) - Safeguarding classified information (last amended 2023-04-05)

• § 117.15(h)(3) - Safeguarding classified information (last amended 2023-04-05)

Part 117 treats the MFO home office and its branches as an entity-eligibility structure: the home office must be eligible at the highest level held in the MFO, and DCSA determines whether a branch needing access is eligible. The GCA provides the contract security classification specification or equivalent and the contractor complies with it. Within the same MFO, a contractor may disclose classified information to its own cleared employees only when they have the required eligibility and need to know and the disclosure is necessary for tasks or services essential to a classified contract or subcontract. Parent-subsidiary disclosure is a different rule and requires separate entity eligibility determinations and appropriate classification guidance.

Required practice

#	Basis	Source	Required action
1	Rule [Entity eligibility]	32 CFR 117.9(i)	Confirm the home office holds entity eligibility at the level required for the MFO and that DCSA has determined the branch eligible when that branch needs access.
2	Rule [Contract guidance]	32 CFR 117.13(d)	Use the GCA-provided contract security classification specification or equivalent as the contract-specific source of classification guidance and comply with all of its applicable terms.
3	Rule [Disclosure]	32 CFR 117.15(h)(1)	Disclose classified information across the MFO only to cleared employees with the appropriate eligibility and need to know, and only as necessary for tasks or services essential to the classified contract or subcontract.
4	Rule [Separate legal entities]	32 CFR 117.15(h)(3)	Treat a parent and subsidiary as separate entities: verify eligibility for both, need to know, the agreement or procurement action requiring disclosure, and approved storage capability when classified material is physically transferred.
5	DCSA guidance [MFO boundary]	DCSA FCL Orientation Handbook, March 2021	Use DD Form 441-1 to identify the cleared divisions and branches covered by the home office security agreement, and distinguish same-entity branches from parents, subsidiaries, affiliates, joint ventures, and other legal entities.
6	DCSA guidance [Location review]	VOI November 2023	Do not assume that clearance of an MFO location, by itself, requires a DD Form 254 revision. Check the DD Form 441-1 performance-location structure and elevate ambiguity to the assigned ISR and Field Office Chief.
7	DCSA guidance [Current DD254 execution]	DCSA DD Form 254 Instructions, updated July 11, 2025	List every location at which the contract defines classified performance in Item 8. For Item 11c work at a division or branch, complete Item 8 for the actual performance location and classification level.

#	Basis	Source	Required action
8	DCSA guidance [Current entity scope]	DCSA SMO Slick Sheet, Version 2.0, November 2025	Apply the current scope boundary: an MFO is one legal entity with the home office on DD Form 441 and cleared branches or divisions on DD Form 441-1; a parent-subsidiary relationship is not an MFO.

Decision paths - which facts point where

Scenario	If	Then
Same legal entity; branch or division performs classified work	The location is a branch or division of the same legal entity, is carried on the DD Form 441-1 as applicable, and will perform work requiring access to classified information.	1. Confirm DCSA entity eligibility and safeguarding capability for the location as the facts require. 2. Confirm employee eligibility, access, and need to know for the contract work. 3. Compare the contract, DD Form 254 Item 8, Item 11 selections, and DD Form 441-1. 4. If Item 11c applies, ensure Item 8 identifies the actual branch or division performance location and classification level. 5. If the documents conflict or the location is omitted, obtain ISR and GCA clarification before treating the location as approved. Use the MFO location only within the contract's classified-performance scope and after the eligibility, need-to-know, safeguarding, and location records align.
Cleared MFO location is absent from the DD Form 254	The branch or division is cleared and belongs to the same legal entity, but the DD Form 254 does not list it as a classified performance location.	1. Do not conclude that clearance alone authorizes contract performance at the location. 2. Determine whether the contract actually defines classified performance at that location. 3. Apply the current Item 8 instructions where the contract defines the location. 4. Use the November 2023 VOI only for its narrow statement that a DD Form 254 update is not automatically required in every such situation. 5. Ask the ISR, Field Office Chief, and GCA to resolve any remaining ambiguity. Do not self-authorize the omitted location; document the government clarification that supports the chosen treatment.
Parent, subsidiary, affiliate, or another legal entity	The proposed performance or disclosure crosses a legal-entity boundary rather than remaining within one MFO.	1. Do not apply the MFO shortcut or the DD Form 441-1 branch structure. 2. Apply the separate Part 117 rule for parent-subsidiary or subcontractor disclosure, as applicable. 3. Verify the other entity's eligibility, need to know, classification guidance, and storage approval when material is transferred. 4. Confirm the governing contract, subcontract, agreement, and DD Form 254 treatment. Handle the recipient as a separate entity and obtain the contract and security authorizations required for that relationship.

Matters not addressed by the regulation

• Neither Part 117 nor the November 2023 VOI says that a DD Form 254 can simply be 'shared' throughout an MFO. The official language addresses disclosure to eligible employees, DD Form 441-1 coverage, and approved performance locations.

• A cleared location is not automatically an approved performance location for every classified contract.

• The November 2023 phrase 'does not necessarily require an update' is not a prohibition on updates and does not override the current Item 8 instructions or the GCA's contract-specific decision.

• MFO treatment stops at the legal-entity boundary. A parent, subsidiary, affiliate, joint venture, or subcontractor is not converted into an MFO branch merely because it belongs to the same corporate family.

• MFO status never removes employee eligibility, access, need-to-know, safeguarding, classification-guidance, or physical-transfer controls.

Guidance changed in the preceding year

Date	Level	Source	Direction and effect	Status / basis
2023-11-01	VOI	VOI November 2023	DCSA states that a cleared MFO location omitted from a DD Form 254 does not necessarily require a DD Form 254 update; it points to DD Form 441-1 for MFO performance locations and directs unresolved ambiguity to the ISR and Field Office Chief.	active; No supersession conclusion
2025-07-11	GUIDANCE	DCSA Instructions for Completing DD Form 254	The current DCSA instructions require Item 8 to list every location at which the contract defines classified performance.	active; No supersession conclusion
2025-07-11	GUIDANCE	DCSA Instructions for Completing DD Form 254	For Item 11c work, the current DCSA instructions require Item 8 completion when a division or branch of the awarded contractor will receive, store, or generate classified information, including the applicable classification level.	active; No supersession conclusion
2025-11-01	GUIDANCE	DCSA SMO Slick Sheet, Version 2.0	DCSA's current MFO job aid defines an MFO as one legal entity with a home office on DD Form 441 and at least one cleared branch or division on DD Form 441-1.	active; No supersession conclusion
2025-11-01	GUIDANCE	DCSA SMO Slick Sheet, Version 2.0	DCSA states that a parent-subsidiary relationship is not an MFO because the parent and subsidiary are separate legal entities executing separate DD Forms 441.	active; No supersession conclusion

Reviewer note: If the DD Form 254, DD Form 441-1, contract statement of work, and actual performance locations do not align, preserve the discrepancy and obtain a documented ISR/GCA resolution; do not infer blanket permission from the VOI.

3.14 § 117.7(l) - NAESOC oversight team verification for newly transitioned facilities

Current-cycle finding: NAESOC continues welcoming new facilities with rolling migrations. The VOI warns that Government Services Portal accounts inactive for over 30 days are automatically locked and directs users to ServiceNow Helpdesk at 878-274-1003 for regaining access. Detected or announced in: VOI October 2026 (2026-10-30). Operational basis: VOI August 2026. The CFR remains

controlling.

What DCSA guidance adds to the rule

The August 2026 VOI supplies the operational verification procedure for facilities that receive a NAESOC reassignment: confirm the oversight team in NISS and use the NAESOC Helpdesk after the reassignment is shown.

Regulatory text - controlling authority

Section 117.7(l) requires notification when NISP oversight is delegated to a cognizant security organization. The rule establishes the oversight relationship; it does not prescribe the NISS verification steps or help-desk channel.

Required practice

#	Basis	Source	Required action
1	DCSA guidance [Verification]	VOI August 2026	If your facility received a NAESOC transition/reassignment notification, log into NISS, confirm your facility profile's oversight team shows “NAESOC,” and direct future inquiries to the NAESOC Helpdesk.

Matters not addressed by the regulation

• This applies only to facilities that actually received a NAESOC transition notification — it is not a general-population action item.

Guidance changed in the preceding year

Date	Level	Source	Direction and effect	Status / basis
2026-08-31	VOI	VOI August 2026	Facilities newly assigned to NAESOC oversight should verify in NISS that their assigned oversight team shows “NAESOC” and then direct future inquiries, administrative updates, and safeguarding support to the NAESOC Helpdesk rather than a prior oversight contact.	active; No supersession conclusion
2026-10-30	VOI	VOI October 2026	NAESOC continues welcoming new facilities with rolling migrations. The VOI warns that Government Services Portal accounts inactive for over 30 days are automatically locked and directs users to ServiceNow Helpdesk at 878-274-1003 for regaining access.	active; No supersession conclusion

Reviewer note: Scope is limited to facilities mid-transition; do not present this as a universal FSO action item.

3.15 § 117.15(c), § 117.15(b) - Open Storage Areas (formerly Closed Areas)

Current-cycle finding: USW(I&S) published administrative guidance on Black Label container phase-out. Authorized uses: internal need-to-know separation within approved open-storage areas and routine combination-lock changes. Explicitly prohibited: primary classified storage outside approved open-storage facilities, and any physical maintenance, structural repair, or locksmith drilling. Mandatory actions: de-label and re-identify with 'No Longer GSA Approved' sticker; replace on mechanical failure with Red Label container; complete retirement from classified operations by October 1, 2028. Detected or announced in: VOI October 2026 (2026-10-30). Operational basis: 32 CFR 117.15(c); VOI Apr 2023; VOI Sep 2022; VOI Jun 2025; VOI Dec 2025; VOI Nov 2024; VOI August 2026 / ISOO Notice 2022-03; VOI August 2026 / GSA-IACSE / DoD Lock Program. The CFR remains controlling.

What DCSA guidance adds to the rule

The rule permits GSA containers, vaults built to FED-STD 832, or open storage areas built to 32 CFR 2001.53 and approved by the CSA. Guidance supplies the approval instrument and two schedules the rule does not contain: DCSA Form 147 with version control, the 1 October 2027 suspense for redocumenting legacy spaces, contractor self-approval authority effective 1 January 2026 which the rule does not provide for, and the treatment of decommissioned black label containers. The VOI restates per-model authorized-use end dates for black label containers (October 2024 through October 2028) and confirms vault doors remain authorized for classified storage until 1 October 2035 under ISOO Notice 2022-03. It also lays out the decommissioning and disposal procedure for containers past their end-of-service date. In October 2026, USW(I&S) published administrative guidance clarifying authorized uses (internal need-to-know separation in approved open-storage areas, routine lock changes) and explicit prohibitions (primary classified storage outside approved open-storage, any maintenance/repair/drilling). Mandatory actions: de-label and re-identify with 'No Longer GSA Approved' sticker; immediate decommission and Red Label replacement on mechanical failure.

Regulatory text - controlling authority

• § 117.15(c) - Safeguarding classified information (last amended 2023-04-05)

Classified information is stored in GSA-approved security containers, in vaults built to Federal Standard 832, or in open storage areas constructed to 32 CFR 2001.53 and approved by the CSA. The rule contains no self-approval authority for contractors.

Required practice

#	Basis	Source	Required action
1	Rule	32 CFR 117.15(c)	Store classified in a GSA-approved container, a vault built to FED-STD 832, or an open storage area built to 32 CFR 2001.53.
2	DCSA guidance	VOI Apr 2023	Use the construct open storage area. Closed areas are obsolete under the NISPOM Rule; existing approved closed areas remain approved until converted.
3	DCSA guidance	VOI Sep 2022	Complete a DCSA Form 147 for each open storage area and treat it as a living record. It becomes the record of approval only when signed by a DCSA ISR.
4	DCSA guidance	VOI Jun 2025	Use only the January 2025 version of DCSA Form 147 from 1 October 2025.
5	DCSA guidance	VOI Jun 2025	For any space still approved on the obsolete one-page Form 147, submit a new Form 147 to redocument it no later than 1 October 2027.
6	DCSA guidance	VOI Dec 2025	From 1 January 2026 you may request self-approval authority for open storage areas. Participation is voluntary; DCSA retains review authority.
7	DCSA guidance	VOI Nov 2024	Decommission all black label containers even if you keep using them. A decommissioned container may still hold classified inside an approved open storage area, because the area's own controls carry the protection. Work to the ISOO Notice 2021-01 schedule, not to your review cycle.
8	DCSA guidance [Authorization check]	VOI August 2026 / ISOO Notice 2022-03	Check any black label GSA security container or vault door against its manufacturer's label (manufacturer, model, serial number, date of manufacture, federal specification) and the published end-of-service table before continuing to rely on it for classified storage; vault doors remain authorized until 1 October 2035.
9	DCSA guidance [Decommissioning and disposal]	VOI August 2026 / GSA-IACSE / DoD Lock Program	For a container past its end-of-service date: search it for and remove all classified material, strip GSA-approval and identification labels, and either mark it for unclassified filing-cabinet use only or follow the disposal procedure (remove/destroy or return limited-use combination locks, then recycle — do not resell).

Matters not addressed by the regulation

• Self-approval authority has changed twice, and neither change appears in the rule. Contractors previously held CSA-granted self-approval authority for closed areas under the legacy NISPOM. 32 CFR Part 117 did not carry it forward, and DCSA's May 2022 guidance stated that contractors have no self-approval authority. Procedures effective 1 January 2026 make self-approval available again on a voluntary basis.

• The term “closed area” remains in circulation in older material. The construct in the current rule is the open storage area built to 32 CFR 2001.53.

• DCSA describes the Form 147 process as replacing obsolete requirements rather than adding new ones. It is a re-documentation exercise rather than a new safeguarding obligation.

• Decommissioning and disposal are distinct. A decommissioned container loses its GSA approval but may remain in service, including for classified material inside an approved open storage area, where the area's own controls provide the protection.

• A container's decommissioning removes authorization for classified storage but does not by itself require disposal — continued unclassified use is permitted if properly marked.

• Vault doors are on a different (later) extended timeline than filing-cabinet-style containers; do not apply the 2035 vault-door date to non-vault-door containers.

Guidance changed in the preceding year

Date	Level	Source	Direction and effect	Status / basis
2022-05-01	VOI	VOI May 2022	Introduced DCSA Form 147 and stated plainly that contractors have no self-approval authority.	active; No supersession conclusion
2025-06-01	VOI	VOI Jun 2025	Announced the return of industry self-certification for open storage areas, targeting 1 October 2025.	superseded; INFERRED - Slipped — see below.
2025-11-01	VOI	VOI Nov 2025	Moved self-approval implementation from 1 October 2025 to 1 January 2026.	superseded; INFERRED - Superseded by the December 2025 issue confirming the effective date.
2025-12	VOI	VOI Dec 2025	From 1 January 2026 you may request self-approval authority for open storage areas. Participation is voluntary; DCSA retains review authority.	active; No supersession conclusion
2026-08-31	VOI	VOI August 2026	Reiterates the black label GSA container phase-out schedule (authorization to use for classified storage ends per container class/model, October 2024 through October 2028) and that vault doors remain authorized for classified storage until 1 October 2035 per an ISOO extension.	active; No supersession conclusion

Date	Level	Source	Direction and effect	Status / basis
2026-08-31	VOI	VOI August 2026	Sets out the required steps once a black label container reaches end of service: search for and remove all classified material, remove GSA-approval and identification labels, mark the container as no longer GSA approved for continued unclassified filing-cabinet use, or follow the separate disposal procedure (remove/destroy or return limited-use combination locks, and recycle rather than resell) if the container is being disposed of.	active; No supersession conclusion
2026-08-31	GUIDANCE	ISOO Notice 2026-06	Expressly rescinds and replaces ISOO Notices 2022-03 and 2021-01, retains the current black-label equipment deadlines, and consolidates the disposal procedure.	active; EXPLICIT - "This Notice rescinds and replaces ISOO Notices 2022-03 and 2021-01." (ISOO Notice 2026-06, PDF p. 1)
2026-10-30	VOI	VOI October 2026	USW(I&S) published administrative guidance on Black Label container phase-out. Authorized uses: internal need-to-know separation within approved open-storage areas and routine combination-lock changes. Explicitly prohibited: primary classified storage outside approved open-storage facilities, and any physical maintenance, structural repair, or locksmith drilling. Mandatory actions: de-label and re-identify with 'No Longer GSA Approved' sticker; replace on mechanical failure with Red Label container; complete retirement from classified operations by October 1, 2028.	active; No supersession conclusion

Reviewer note: ISOO Notice 2026-06 is the current external authority. Its official PDF has been validated in governed quarantine but has not yet been promoted into the active DCSA Library.

3.16 § 117.10(b)(5) - Reinvestigation and Continuous Vetting

Current-cycle finding: Current. Periodic reinvestigations are no longer required; submit a PVQ every five years, timed from the DISS PVQ Date. Detected or announced in: VOI May 2026 (2026-05-01). Operational basis: VOI May 2026; VOI Mar 2026; VOI Dec 2016; 32 CFR 117.10(b)(5). The CFR remains controlling.

What DCSA guidance adds to the rule

The rule directs contractors to follow CSA guidance and sets no interval of any kind. Every operative element comes from guidance: that periodic reinvestigations are no longer required, the five-year Personnel Vetting Questionnaire cycle applying regardless of eligibility level, timing from the DISS PVQ Date field rather than the investigation close date, and the NBIS order form selection. If that guidance changed, the rule would supply no fallback.

Regulatory text - controlling authority

• § 117.10(b)(5) - Determination of eligibility for access to classified information for contractor employees (last amended 2021-02-26)

Contractor employees determined eligible for access will follow CSA guidance to complete reinvestigation and continuous evaluation or continuous vetting requirements. The contractor validates that the employee requires continued eligibility before initiating the reinvestigation. The rule delegates the substance to CSA guidance and sets no periodicity.

Required practice

#	Basis	Source	Required action
1	DCSA guidance	VOI May 2026	Periodic reinvestigations are no longer required for NISP contractors.
2	DCSA guidance	VOI May 2026	Submit an updated Personnel Vetting Questionnaire — or an SF-86 via eApp with releases — every five years for each individual, regardless of eligibility level.
3	DCSA guidance	VOI May 2026	Time the submission from the PVQ Date field in DISS.
4	DCSA guidance	VOI Mar 2026	In the NBIS Order Form select “5 year update” as the Investigative Requirement rather than “Reinvestigation”, unless a Government authority directs otherwise, and retain “CV Update” in the Contract Number field.
5	DCSA guidance	VOI Dec 2016	Access is not to be denied or withheld solely because an investigation is out of scope. This rests on the OUSD(I) memorandum of 7 December 2016.
6	Rule	32 CFR 117.10(b)(5)	Validate that the employee requires continued eligibility before initiating a reinvestigation.

Matters not addressed by the regulation

• §117.10(b)(5) sets no periodicity. It provides that contractors follow CSA guidance. The five-year cycle and the PVQ instrument therefore rest on the May 2026 article rather than on the rule, and the rule provides no fallback interval.

• The rule continues to use the term “reinvestigation”. A schedule built from the rule text alone would key to investigation anniversaries rather than to the PVQ Date field.

• Eligibility does not lapse with the investigation. The December 2016 memorandum provides that access is not denied solely because an investigation is out of scope.

• The five-year cycle is stated to apply regardless of eligibility level, without the tier distinction that previously governed submission intervals.

Guidance changed in the preceding year

Date	Level	Source	Direction and effect	Status / basis
2018-07-01	VOI	VOI Jul 2018	Under DNI and OPM backlog mitigation, contractors continued to submit at six years (T5R) and ten years (T3R); DCSA applied a risk-based screen and could defer a request, enrolling the subject into continuous evaluation.	superseded; INFERRED - The deferral model bridged periodic reinvestigation and continuous vetting. Superseded by the 2026 PVQ cycle.
2026-03-31	VOI	VOI Mar 2026	In the NBIS Order Form select “5 year update” as the Investigative Requirement rather than “Reinvestigation”, unless a Government authority directs otherwise, and retain “CV Update” in the Contract Number field.	active; No supersession conclusion
2026-05-01	VOI	VOI May 2026	Current. Periodic reinvestigations are no longer required; submit a PVQ every five years, timed from the DISS PVQ Date.	active; No supersession conclusion

Reviewer note: Continuous Vetting enrolment is a separate obligation running alongside the PVQ cycle. Where a KMP holds eligibility without access — an ITPSO with no need for access, for example — the December 2025 guidance provides for maintaining the DISS record, continuing CV enrolment, and submitting the five-year update.

3.17 § 117.8, § 117.7(h)(2)(i), § 117.7(h)(2)(ii), § 117.7(h)(2)(iii) - Reporting Requirements and SEAD 3 Reportable Activities

Current-cycle finding: DCSA reminds facilities to ensure the SMO certifies the self-inspection and that completion is annotated in NISS. Detected or announced in: VOI September 2026 (2026-09-30). Operational basis: 32 CFR 117.8(a)(2); ISL 2021-02; VOI Jan 2025; 32 CFR 117.8(a) / SEAD 3; VOI Mar 2025; 32 CFR 117.8(c)(1); 32 CFR 117.8(c)(1)(i); 32 CFR 117.8(e); 32 CFR 117.8(c)(2); SEAD 3 E. and F.; SEAD 3 F.1.b.1); SEAD 3 D.8, F.1.a, F.2.a; SEAD 3 H.1 and H.2; 32 CFR 117.8(c)(3); 32 CFR 117.8(c)(4); 32 CFR 117.8(c)(5); 32 CFR 117.8(c)(6); 32 CFR 117.8(c)(7); VOI Jan 2022; VOI Jul 2026; 32 CFR 117.8(c)(8); 32 CFR 117.8(c)(9); 32 CFR 117.8(c)(10) and (c)(14); 32 CFR 117.8(c)(11); 32 CFR 117.8(c)(12); 32 CFR 117.8(c)(13); 32 CFR 117.8(b); 32 CFR 117.8(d); 32 CFR 117.8(f); 32 CFR 117.8(g); VOI August 2026; 32 CFR 117.7(h)(2)(iii); VOI September 2026. The CFR remains controlling.

What DCSA guidance adds to the rule

The rule sets out a long list of reports in its own right — adverse information, suspicious contacts, employee status changes, entity changed conditions, storage and safeguarding failures, loss or compromise, CDC cyber incidents and reports to ISOO. What it does not contain is the catalogue of what an individual reports about themselves. §117.8(a) incorporates SEAD 3 by reference for that, and ISL 2021-02 applies it to cleared industry: the four steps that make foreign travel deemed pre-approved, the five-business-day and 120-day rules, the separate CISA notification for foreign intelligence entity contact, and the expanded set at Top Secret or Q. Two categories — cryptocurrency and psychological health — come from the ISL alone and bind only entities under DoD cognizance. The rule also names no system: DISS and the NISS changed-condition package both come from guidance. §117.8 has not been substantively amended since 24 February 2021. During a facility's FCL anniversary month, DCSA sends the Annual Industry Check-Up Tool to help identify outstanding reporting under Part 117; it is explicitly not a substitute for the required self-inspection.

Regulatory text - controlling authority

• § 117.8 - Reporting requirements (last amended 2023-04-05)

Contractors and cleared employees report events affecting eligibility, events indicating an insider threat, events affecting safeguarding, and known or suspected loss or compromise. The contractor establishes internal procedures so employees know what to report to the FSO. Espionage, sabotage, terrorism and subversive activity go to the nearest FBI field office, with the CSA notified and given a copy. Adverse information, suspicious contacts, changes in employee status and changed conditions affecting the entity go to the CSA. Loss or compromise triggers a preliminary inquiry, an initial report and a final report. Contractors will not make reports based on rumor or innuendo. The rule points to SEAD 3 and CSA-provided guidance for what is reportable; it does not reproduce the list.

Required practice

#	Basis	Source	Required action
1	Rule [Program, scope and channel]	32 CFR 117.8(a)(2)	Establish internal procedures to ensure employees with eligibility for access are aware of their responsibilities for reporting pertinent information to the FSO.

#	Basis	Source	Required action
2	Binding DCSA supplementary procedures [Program, scope and channel]	ISL 2021-02	Maintain a written plan or standard practice procedure implementing SEAD 3. It must cover how you receive, process and manage covered-individual reports, how the procedures are implemented at the facility, and how a covered individual alerts you to reportable activity by other covered individuals (SEAD 3 F.3).
3	DCSA guidance [Program, scope and channel]	VOI Jan 2025	Have that written procedure ready to produce at every scheduled security review, including remote reviews.
4	Incorporated authority [Program, scope and channel]	32 CFR 117.8(a) / SEAD 3	SEAD 3 is incorporated by the rule itself, not merely applied by ISL 2021-02. §117.8(a) requires reporting "pursuant to this rule, SEAD 3 … and CSA-provided guidance". The reportable activities below marked [I] would survive withdrawal of the ISL.
5	Binding DCSA supplementary procedures [Program, scope and channel]	ISL 2021-02	"Covered individuals" means only personnel granted eligibility for access through the NISP, or in process for it. Uncleared personnel subject to SEAD 3 solely because they occupy a sensitive position are not covered by the NISP or by this ISL, and go to their Government customer.
6	Binding DCSA supplementary procedures [Program, scope and channel]	ISL 2021-02	Submit required personnel reports through the DoD-designated system of record, currently DISS. Information already submitted on an SF-86 or in DISS is not resubmitted.
7	DCSA guidance [Program, scope and channel]	VOI Mar 2025	Submit all known reportable information before out-processing a subject from your DISS SMO. If it is missed, re-establish affiliation, submit the report, then out-process again.
8	Rule [Personnel — adverse information and conduct]	32 CFR 117.8(c)(1)	Report adverse information coming to your attention concerning any employee determined eligible for access. Do not make reports based on rumor or innuendo.
9	Rule [Personnel — adverse information and conduct]	32 CFR 117.8(c)(1)(i)	Termination of employment does not negate the requirement to submit the report. Where the employee is assigned to a USG location, furnish a copy of the report and its final disposition to that location's security point of contact.
10	Binding DCSA supplementary procedures [Personnel — adverse information and conduct]	ISL 2021-02	Report adverse information for the full duration of employment. An anticipated or imminent departure does not change the duty. For adverse information about employees who have already left, contact DCSA for guidance.
11	Binding DCSA supplementary procedures [Personnel — adverse information and conduct]	ISL 2021-02	Base adverse information reporting on the 13 adjudicative guidelines in SEAD 4.
12	Rule [Personnel — adverse information and conduct]	32 CFR 117.8(e)	Establish and enforce policies for administrative or disciplinary action against employees who violate the rule; maintain a system to track violations so patterns of negligence or a potential insider threat can be identified; apply a graduated scale of action; and submit a final culpability report to the CSA stating the action taken and whether the violation involved deliberate disregard, negligence, or a pattern of questionable judgment.
13	Rule [Personnel — foreign travel, contacts and finances]	32 CFR 117.8(c)(2)	Report suspicious contacts: efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to your cleared facility; efforts to elicit information from a cleared employee; and any contact suggesting the employee may be the target of attempted exploitation by a foreign intelligence service. The rule directs you to SEAD 3 for the specific information to be reported.
14	Incorporated authority [Personnel — foreign travel, contacts and finances]	SEAD 3 E. and F.	For unofficial foreign travel to be deemed pre-approved, all four must occur: the employee notifies you before travel; you receive and report a complete itinerary in DISS before travel; you give the traveller the NCSC Safe Travels resource for required review; and you coordinate with your DCSA CISA for a pre-travel briefing where the destination appears in the DNI Worldwide Threat Assessment.
15	Incorporated authority [Personnel — foreign travel, contacts and finances]	SEAD 3 F.1.b.1)	Capture itinerary deviations, unplanned Canada or Mexico day trips, and emergency travel within five business days of return. Aggregated travel reporting must not span more than 120 days, and where it is used, refer the traveller to the NCSC Safe Travels resource at least annually.
16	Binding DCSA supplementary procedures [Personnel — foreign travel, contacts and finances]	ISL 2021-02	Unofficial contact with a known or suspected foreign intelligence entity requires a DISS customer service report and a direct report to your facility's DCSA CISA. Coordinate post-travel debriefings with the CISA where a traveller reports FIE contact or travel anomalies.
17	Incorporated authority [Personnel — foreign travel, contacts and finances]	SEAD 3 D.8, F.1.a, F.2.a	Not reportable: contact with foreign nationals arising solely from official duties or from residing abroad for employment, absent bonds of affection or obligation; and official foreign travel in direct support of a U.S. Government contract. Official foreign contact you deem a security concern still requires a DISS incident report.

#	Basis	Source	Required action
18	Binding DCSA supplementary procedures [Personnel — foreign travel, contacts and finances]	ISL 2021-02	Cryptocurrency: report foreign state-backed, hosted or managed cryptocurrency, and wallets hosted by foreign exchanges, with the currency name, exchange host country and dollar value. No report where the individual is unaware of any foreign connection, or where holdings sit in a widely diversified fund unless that fund is entirely composed of such cryptocurrency. This category comes from the ISL, not from SEAD 3 — it binds only entities under DoD cognizance.
19	Binding DCSA supplementary procedures [Personnel — foreign travel, contacts and finances]	ISL 2021-02	Psychological and emotional health: report only the six situations aligned to SF-86 Section 21 — an order declaring mental incompetency, a court-ordered consultation with a mental health professional, hospitalization for a mental health condition, diagnosis of a listed disorder, altering or discontinuing treatment for one of those diagnoses within the last seven years without consulting a professional, and any condition the individual believes substantially and adversely affects judgment, reliability or trustworthiness. This category comes from the ISL, not from SEAD 3.
20	Incorporated authority [Personnel — foreign travel, contacts and finances]	SEAD 3 H.1 and H.2	Top Secret or Q access adds: foreign voting, financial anomalies including any unusual infusion of assets of $10,000 or greater, direct foreign business involvement, foreign bank accounts, foreign property ownership including timeshares and natural resource rights, cohabitants, marriage, adoption of non-U.S.-citizen children, and foreign national roommates.
21	Rule [Employee status and eligibility events]	32 CFR 117.8(c)(3)	Report changes in status of employees determined eligible for access: death, change in name, termination of employment, and change in citizenship, by the CSA-designated reporting mechanism.
22	Rule [Employee status and eligibility events]	32 CFR 117.8(c)(4)	Where a non-U.S. citizen employee granted an LAA becomes a citizen through naturalization, report the city, county and state where naturalized, the date, the court, and the certificate number.
23	Rule [Employee status and eligibility events]	32 CFR 117.8(c)(5)	Report when an employee no longer wishes to be processed for eligibility or to continue having access, and the reason for the request.
24	Rule [Employee status and eligibility events]	32 CFR 117.8(c)(6)	Report an employee's refusal to sign the SF 312 or other approved NDA. Access is denied under §117.10(g)(4).
25	Rule [Entity and facility conditions]	32 CFR 117.8(c)(7)	Report changed conditions affecting entity eligibility: change of ownership or control including stock transfers; change of operating name or address; any change to previously submitted KMP information, with a statement whether the new KMP are cleared and at what level, or excluded under §117.7(b)(5)(ii) or temporarily excluded under §117.9(g); action to terminate business or imminent bankruptcy or reorganization; and any material change to previously reported FOCI, by submitting an updated SF 328.
26	DCSA guidance [Entity and facility conditions]	VOI Jan 2022	Submit changed conditions to DCSA through a NISS Change Condition package; the user guide is in the NISS Knowledge Base.
27	DCSA guidance [Entity and facility conditions]	VOI Jul 2026	Review your NISS facility profile: confirm KMP listings with current contact information and clearance status, verify FSO and ITPSO email and phone so DCSA correspondence is not missed, and promptly report ownership transitions, joint ventures and address changes.
28	Rule [Entity and facility conditions]	32 CFR 117.8(c)(8)	Report any change in your storage requirement or capability to safeguard classified material.
29	Rule [Entity and facility conditions]	32 CFR 117.8(c)(9)	Report any emergency situation that renders the location incapable of safeguarding classified material as soon as possible.
30	Rule [Entity and facility conditions]	32 CFR 117.8(c)(10) and (c)(14)	Report information indicating a subcontractor cannot adequately protect classified information, or circumstances affecting the validity of its eligibility — and, as a subcontractor, the same about your prime. Subcontractors also notify their prime whenever they make a report under (c)(7) through (c)(10).
31	Rule [Entity and facility conditions]	32 CFR 117.8(c)(11)	Report when the location or disposition of material previously terminated from accountability is later discovered and brought back into accountability.
32	Rule [Entity and facility conditions]	32 CFR 117.8(c)(12)	Report any pre-contract negotiation or award not placed through a CSA or U.S. GCA that involves, or may involve, release of U.S. classified information to a foreign interest or access to classified information furnished by a foreign interest.
33	Rule [Entity and facility conditions]	32 CFR 117.8(c)(13)	Report receipt of classified material from foreign interests that did not come through USG channels.
34	Rule [Espionage, loss, cyber and ISOO]	32 CFR 117.8(b)	Promptly submit a written report to the nearest FBI field office on actual, probable or possible espionage, sabotage, terrorism or subversive activities at any of your locations. An initial report may be made by phone but must be followed up in writing regardless of the FBI's disposition, and you must promptly notify the CSA and give it a copy of the written report.
35	Rule [Espionage, loss, cyber and ISOO]	32 CFR 117.8(d)	On any loss, compromise or suspected compromise of classified information, U.S. or foreign: immediately initiate a preliminary inquiry including validation of the classification; submit an initial report if the inquiry confirms an incident, unless the CSA notifies otherwise; and submit a final report on completion with the responsible individual's full name and SSN, prior incident record, corrective action, disciplinary action, and the specific reasons for the conclusion reached.
36	Rule [Espionage, loss, cyber and ISOO]	32 CFR 117.8(f)	Cleared defense contractors only. Immediately report to the designated DoD CSO any cyber incident on a classified covered information system that CSO has approved, including the technique or method used, a sample of the malicious software if isolated, and a summary of any DoD program potentially compromised. Allow DoD personnel access to equipment and information needed for forensic analysis on request.
37	Rule [Espionage, loss, cyber and ISOO]	32 CFR 117.8(g)	Report to the Director, ISOO instances of redundant or duplicative security review or audit activity by CSAs, and instances of a CSA duplicating processing of an entity eligibility determination another CSA has already made.

#	Basis	Source	Required action
38	Binding DCSA supplementary procedures [Espionage, loss, cyber and ISOO]	ISL 2021-02	Stop citing ISL 2011-04 for adverse information reporting examples. This ISL cancels, incorporates and rescinds it.
39	DCSA guidance [Reporting check]	VOI August 2026	Use the Annual Industry Check-Up Tool sent during your FCL anniversary month to help identify outstanding 32 CFR Part 117 reporting, but do not treat it as satisfying your annual self-inspection requirement.
40	Rule [Self-inspection certification]	32 CFR 117.7(h)(2)(iii)	Have the SMO annually certify in writing that the self-inspection was conducted, other KMP were briefed, appropriate corrective actions were taken, and management supports the security program.
41	DCSA guidance [NISS completion record]	VOI September 2026	After the SMO certification, annotate the self-inspection as complete in NISS.

Matters not addressed by the regulation

• SEAD 3 is incorporated by the rule, not merely applied by an ISL. §117.8(a) requires reporting “pursuant to this rule, SEAD 3 … and CSA-provided guidance”, and §117.8(c)(2) points to SEAD 3 for the specific information to report. Steps marked [I] rest on that incorporation and would survive withdrawal of ISL 2021-02. Steps marked [G] would not.

• Two reportable categories are industry-only. Cryptocurrency and psychological health come from ISL 2021-02 rather than from SEAD 3. ISLs bind only entities for which the Department of Defense is the Cognizant Security Agency, so contractors under a different CSA do not inherit them.

• “Covered individual” is narrower than “employee”. ISL 2021-02 limits it to those granted eligibility or in process for it. An uncleared person in a sensitive position is not your reporting burden and goes to their Government customer.

• Not every report goes to the CSA. Espionage, sabotage, terrorism and subversive activity go to the FBI with a copy to the CSA; foreign intelligence entity contact also goes directly to your CISA; CDC cyber incidents go to the DoD CSO; duplicative review activity goes to ISOO. The DISS report does not discharge any of these.

• The rule names no reporting system. DISS as the personnel channel, and the NISS changed-condition package for entity changes, are both set by guidance rather than by §117.8.

• Foreign travel pre-approval is a four-part test, not a notification. All four steps must occur for the travel to be deemed approved. Completing three leaves the travel unapproved.

• Two ISL 2021-02 items are spent. The 24 August 2021 compliance date and the 18-month extension for foreign travel reporting have both run. A procedure that still recites them is quoting an expired transition.

• The Check-Up Tool is explicitly stated not to replace or count as the self-inspection — do not conflate the two.

Guidance changed in the preceding year

Date	Level	Source	Direction and effect	Status / basis
2024-05-01	ISL	ISL 2021-02	Reissued with two updated reference links: the DCSA CISA field-location lookup and the DNI Worldwide Threat Assessment.	active; No supersession conclusion
2026-07	VOI	VOI Jul 2026	Review your NISS facility profile: confirm KMP listings with current contact information and clearance status, verify FSO and ITPSO email and phone so DCSA correspondence is not missed, and promptly report ownership transitions, joint ventures and address changes.	active; No supersession conclusion
2026-08-31	VOI	VOI August 2026	During a facility's FCL anniversary month, DCSA sends the Annual Industry Check-Up Tool as a reminder to check completion of reporting requirements under 32 CFR Part 117 (NISPOM); the tool does not substitute for the required self-inspection.	active; No supersession conclusion
2026-09-30	VOI	VOI September 2026	DCSA reminds facilities to ensure the SMO certifies the self-inspection and that completion is annotated in NISS.	active; No supersession conclusion

Reviewer note: §117.8(c) was the second most-cited reference in DCSA’s FY25 security review deficiencies, behind only §117.18(b). ISL 2021-02 expressly declines to give guidance on two live questions: whether to report use of CBD products, and whether to report financial holdings in companies dealing in schedule I substances. It warns that unlabeled hemp products can carry enough THC to produce a positive urinalysis and consequent adverse action. Both are open questions for your ISR rather than settled positions.

3.18 § 117.7(h)(2) - Security Rating Score Tool 2.0 and self-inspection alignment

Current-cycle finding: Effective October 1, 2026, DCSA field operations use Security Rating Score Tool 2.0 exclusively for post-review calculations and formal facility ratings; facilities are strongly encouraged to use the finalized resources during annual

self-inspections. Detected or announced in: VOI September 2026 (2026-09-30). Operational basis: 32 CFR 117.7(h)(2); VOI September 2026. The CFR remains controlling.

What DCSA guidance adds to the rule

DCSA field operations use Tool 2.0 exclusively for post-review calculations and formal facility ratings beginning October 1, 2026. Industry is strongly encouraged—not required by this VOI—to use the finalized Tool 2.0 resources during annual self-inspections.

Regulatory text - controlling authority

• § 117.7(h)(2) - Procedures (last amended 2024-07-15)

32 CFR 117.7(h)(2) requires a formal self-inspection at least annually with sufficient scope, depth, management support, documented findings, issue resolution, corrective action, and SMO certification. The rule does not mandate a particular DCSA rating workbook for contractors.

Required practice

#	Basis	Source	Required action
1	Rule [Required self-inspection]	32 CFR 117.7(h)(2)	Conduct and document the annual self-inspection and complete the required management certification and corrective actions.
2	DCSA guidance [Recommended alignment]	VOI September 2026	Use the finalized Security Rating Score Tool 2.0 resources during the annual self-inspection when aligning the facility's self-assessment with DCSA review standards.

Matters not addressed by the regulation

• Mandatory implementation applies to DCSA field operations. The VOI describes industry use as strongly encouraged, not mandatory.

• Using the workbook does not replace the formal self-inspection duties in §117.7(h)(2).

Guidance changed in the preceding year

Date	Level	Source	Direction and effect	Status / basis
2026-09-30	VOI	VOI September 2026	Effective October 1, 2026, DCSA field operations use Security Rating Score Tool 2.0 exclusively for post-review calculations and formal facility ratings; facilities are strongly encouraged to use the finalized resources during annual self-inspections.	active; No supersession conclusion

3.19 § 117.11(b), § 117.11(d) - SF-328 Certificate Pertaining to Foreign Interests — revised form

Current-cycle finding: The SF-328 (Certificate Pertaining to Foreign Interests) has been updated since its May 2025 deployment: condensed to nine questions; SEC filings (Schedules 13D/13G) now retrieved by DCSA rather than submitted by the facility; the separate Statement of Full Disclosure of Foreign Affiliations is retired; Question 1 broadened for diverse foreign ownership structures; Question 4 adds 'binding authority' as a means of foreign control; Question 7b foreign-income threshold set at 15%. The form is the standard certificate for FOCI Expansion, CMMC, and SBIR/STTR programs. Detected or announced in: VOI October 2026 (2026-10-30). Operational basis: VOI October 2026. The CFR remains controlling.

What DCSA guidance adds to the rule

The SF-328 was updated after its May 2025 deployment: condensed to nine questions; DCSA now retrieves SEC filings (Schedules 13D/13G) directly, eliminating that burden; the Statement of Full Disclosure of Foreign Affiliations attachment is retired; Question 1 broadened for diverse ownership; Question 4 adds 'binding authority' as foreign control; Question 7b threshold set at 15% for foreign income. The form is the standard for FOCI Expansion, CMMC, and SBIR/STTR. A new submission is required only for FOCI Expansion, new mission authority, material change, or alignment with new instructions — not solely because the form was updated.

Regulatory text - controlling authority

• § 117.11(b) - Foreign Ownership, Control, or Influence (FOCI) (last amended 2023-04-05)

• § 117.11(d) - Foreign Ownership, Control, or Influence (FOCI) (last amended 2023-04-05)

32 CFR 117.11(b) and (d) require the SF-328 as part of FOCI reporting and mitigation. The form itself is a GSA standard form managed by DCSA.

Required practice

#	Basis	Source	Required action
1	DCSA guidance [Form usage]	VOI October 2026	Use the current SF-328 revision for any new submission. Do not submit a new SF-328 solely because the form was updated.
2	DCSA guidance [Foreign control assessment]	VOI October 2026	When completing Question 4, evaluate whether any foreign entity holds 'binding authority' over the facility, in addition to the traditional ownership and control factors.
3	DCSA guidance [Income reporting]	VOI October 2026	For Question 7b, apply the 15% threshold for foreign-source income reporting.

Decision paths - which facts point where

Scenario	If	Then
You are submitting an SF-328 for FOCI Expansion, new mission	You are submitting an SF-328 for FOCI Expansion, new mission authority, or material change	1. Confirm the reason for the submission: an unclassified contract over $5M under FOCI Expansion, review under a new mission authority, a material change, or an update needed to align the facility's records with the new instructions. 2. Complete the current SF-328 revision. 3. For Question 4, consider "binding authority" as a means of foreign control; for Question 7b, apply the 15 percent foreign income threshold. Use the current revised form; address all nine questions including the new 'binding authority' criterion and 15% income threshold.
Your only reason for a new SF-328 is that the form was updat	Your only reason for a new SF-328 is that the form was updated	1. Confirm none of the submission triggers applies: FOCI Expansion contract over $5M, new mission authority, material change, or alignment with the new instructions. 2. Do not submit a new SF-328 on the form update alone. No submission is required solely for that reason.

Matters not addressed by the regulation

• The removal of the Statement of Full Disclosure does not reduce disclosure obligations; the information is now captured within the nine-question structure.

• 'Binding authority' in Question 4 is a new criterion that was not on earlier versions — do not overlook it.

• The 15% foreign-income threshold in Question 7b is a specific reporting line, not a control threshold.

Guidance changed in the preceding year

Date	Level	Source	Direction and effect	Status / basis
2026-10-30	VOI	VOI October 2026	The SF-328 (Certificate Pertaining to Foreign Interests) has been updated since its May 2025 deployment: condensed to nine questions; SEC filings (Schedules 13D/13G) now retrieved by DCSA rather than submitted by the facility; the separate Statement of Full Disclosure of Foreign Affiliations is retired; Question 1 broadened for diverse foreign ownership structures; Question 4 adds 'binding authority' as a means of foreign control; Question 7b foreign-income threshold set at 15%. The form is the standard certificate for FOCI Expansion, CMMC, and SBIR/STTR programs.	active; No supersession conclusion

Reviewer note: The SF-328 is the standard certificate for FOCI Expansion, CMMC, and SBIR/STTR. Changes to any of these programs may drive further form revisions.

3.20 § 117.10(d) - Submission of the SF 86 (NBIS eApp)

Current operational direction: eApp remains the portal where individuals access and complete their vetting forms, even after investigation request activity moves to DISS. Do not redirect applicants. Source: VOI Jun 2026 (2026-06). This is the newest applicable active guidance recorded for this topic; the CFR remains controlling.

What DCSA guidance adds to the rule

The rule still names e-QIP and provides for “its successor system” without identifying it. ISL 2024-02 identifies the successor — the NBIS Electronic Application (eApp), effective 1 October 2023 — and that identification exists only in guidance. An FSO working from the rule text alone is directed to a system that no longer accepts new initiations. What guidance does not touch is the handling duty: the written notice to the employee and the bar on sharing SF 86 content inside the company are rule obligations with Privacy Act consequences.

Regulatory text - controlling authority

• § 117.10(d) - Determination of eligibility for access to classified information for contractor employees (last amended 2021-02-26)

The electronic version of the SF 86 must be completed in e-QIP or its successor system by the contractor employee and reviewed by the FSO or other contractor employee(s) specifically designated by the contractor to review an employee's SF 86. The FSO or designee will provide the employee written notification that the review is for adequacy and completeness and that the information will be used for no other purpose within the entity, and will not share the information within the entity or use it for any other purpose. The rule names e-QIP and provides for a successor; it does not name that successor.

Required practice

#	Basis	Source	Required action
1	Rule	32 CFR 117.10(d)	The employee completes the electronic SF 86 in e-QIP or its successor system, and the FSO or a specifically designated contractor employee reviews it.
2	Rule	32 CFR 117.10(d)(1)	Give the employee written notification that review of the SF 86 by the FSO or other contractor employee is for adequacy and completeness only, and that the information will be used for no other purpose within the entity. Use and disclosure by the U.S. Government is governed by the Privacy Act of 1974 and the routine uses in the applicable System of Records Notice.
3	Rule	32 CFR 117.10(d)(2)	Do not share information from the employee's SF 86 within the entity, and do not use it for any purpose other than determining the adequacy and completeness of the form.
4	Binding DCSA supplementary procedures	ISL 2024-02	The successor system is the NBIS Electronic Application (eApp), effective 1 October 2023. Submit SF 86 packages through eApp rather than e-QIP.
5	DCSA guidance	VOI Sep 2023	From 1 October 2023 industry uses only NBIS to initiate new investigation requests.
6	DCSA guidance	VOI Nov 2023	eApp signature pages are valid 120 days, the same period as fingerprint results — which is what ties fingerprint submission timing to the request.
7	DCSA guidance	VOI Jun 2026	eApp remains the portal where individuals access and complete their vetting forms, even after investigation request activity moves to DISS. Do not redirect applicants.
8	DCSA guidance	VOI Feb 2017	Review SF 86 packages for accuracy and completeness before submission. The recurring rejection causes are missing fingerprints, incomplete mailing addresses, missing cohabitant or spouse detail, and unverified periods of unemployment or self-employment.
9	DCSA guidance	VOI Dec 2025	Include personal email addresses for every essential KMP in the initial facility clearance package submitted in NISS, so DCSA can initiate the eApp SF 86 request without chasing contact details.

Matters not addressed by the regulation

• The SF 86 review carries a written-notice duty and an internal-sharing bar. §117.10(d)(1) requires written notification to the employee that the review is for adequacy and completeness only; §117.10(d)(2) forbids sharing the content within the entity or using it for any other purpose. Neither is discretionary, and neither appears in any ISL or newsletter.

• The rule names a system that no longer takes submissions. §117.10(d) still says e-QIP. That e-QIP stopped accepting new initiations on 1 October 2023 is stated only in ISL 2024-02 and the 2023 newsletters.

• The review requirement is not the FSO's alone, but the designation must be specific. The rule permits another contractor employee — one specifically designated by the contractor to review employee SF 86s, not merely anyone available.

• The eApp transition was never a DISS replacement. The September 2023 bulletin limited it to Standard Form submissions with no data migration; subject management and visit requests stayed in DISS.

Guidance changed in the preceding year

Date	Level	Source	Direction and effect	Status / basis
2024-05-01	ISL	ISL 2024-02	Formally identified eApp as the successor system to e-QIP for submission of the SF 86 as provided for in §117.10(d).	active; No supersession conclusion
2025-12	VOI	VOI Dec 2025	Include personal email addresses for every essential KMP in the initial facility clearance package submitted in NISS, so DCSA can initiate the eApp SF 86 request without chasing contact details.	active; No supersession conclusion
2026-06	VOI	VOI Jun 2026	eApp remains the portal where individuals access and complete their vetting forms, even after investigation request activity moves to DISS. Do not redirect applicants.	active; No supersession conclusion

Reviewer note: The rule text will keep pointing at e-QIP until Part 117 is amended, and Part 117 has not been substantively amended since 24 February 2021. A procedure that cites §117.10(d) should name eApp explicitly, and should carry the written-notice template required by §117.10(d)(1) — a document an ISR can ask to see.

3.21 § 117.10(c) - Verification of U.S. Citizenship

Current-cycle finding: Evidence may be examined by physical inspection, digital review, or another contractor-managed method. Record in your written procedures which method you use. Detected or announced in: VOI Jul 2026 (2026-07). Operational basis: VOI Feb 2026; VOI Jul 2026; 32 CFR 117.10(c); 32 CFR 117.10(c)(1)-(2); VOI Jan 2026. The CFR remains controlling.

What DCSA guidance adds to the rule

The rule requires evidence of citizenship from each applicant, in original or certified copy, from a listed set of documents. Guidance narrows and qualifies this in three ways: verification is treated as a one-time event at the first Moderate Tier (T3) or High Tier (T4, T5) application rather than at each application; four items that a reader might take as sufficient are identified as not acceptable (Enhanced Driver's License, Form I-551, standard REAL ID, DISS record); and examination may be physical, digital or contractor-managed. The document list itself is unchanged.

Regulatory text - controlling authority

• § 117.10(c) - Determination of eligibility for access to classified information for contractor employees (last amended 2021-02-26)

A contractor will require each applicant for determination of eligibility for access to classified information who claims U.S. citizenship to provide evidence of citizenship to the FSO or other authorized representative. All documentation must be the original or certified copies of the original documents. Paragraph (c)(1) lists documents corroborating citizenship by birth, including by birth abroad to a U.S. citizen; paragraph (c)(2) lists documents corroborating citizenship by certification, naturalization, or birth abroad to a U.S. citizen. A passport appears in both lists.

Required practice

#	Basis	Source	Required action
1	DCSA guidance	VOI Feb 2026	Verification is required in support of an individual's first Moderate Tier (T3) or High Tier (T4, T5) application, before DCSA begins the investigation.
2	DCSA guidance	VOI Jul 2026	Evidence may be examined by physical inspection, digital review, or another contractor-managed method. Record in your written procedures which method you use.
3	Rule	32 CFR 117.10(c)	The documentation itself must be an original or a certified copy.
4	Rule	32 CFR 117.10(c)(1)-(2)	Acceptable documents are those listed in the rule. By birth (§117.10(c)(1)): a birth certificate certified with the registrar's signature bearing the raised, embossed, impressed or multicolored seal of the registrar's office; a current or expired U.S. passport or passport card that is unaltered and undamaged and was originally issued to the individual; Form FS-240; or Form FS-545 or DS-1350. By certification, naturalization or birth abroad (§117.10(c)(2)): Form N-560 or N-561; Naturalization Certificate Form 550, 551 or 570; or a valid or expired U.S. passport or passport card, unaltered and undamaged and originally issued to the individual.
5	DCSA guidance	VOI Jan 2026	DCSA identifies four items as not acceptable proof of citizenship: the Enhanced Driver's License, Form I-551, a standard REAL ID, and a DISS record.
6	DCSA guidance	VOI Feb 2026	Re-verification is not required for subsequent applications once eligibility has been granted — for example a Continuous Vetting eligibility upgrade, or new eligibility after a break in employment.
7	DCSA guidance	VOI Feb 2026	Whether an application is a first application turns on whether eligibility was granted. Where a prior application did not result in eligibility, a subsequent application — including at a new company — is treated as a first application.
8	DCSA guidance	VOI Feb 2026	Re-verification before a subsequent application or before granting access remains permitted but not required. You may also ask a returning employee whether their citizenship status has changed.

Matters not addressed by the regulation

• The one-time reading comes from guidance, not the rule. §117.10(c) refers to each applicant. The February 2026 article states that verification is required in support of a first Moderate Tier (T3) or High Tier (T4, T5) application. Read narrowly, that article addresses MT and HT applications and is not extended here beyond them.

• DISS answers a different question, and the two issues frame it differently. The January 2026 article answers No against DISS in a table of acceptable proof, without qualification. The February 2026 article states that DISS can be used to verify current or previous eligibility but cannot be used to verify citizenship for a first application. Both are consistent on the narrow point — a DISS record is not proof of citizenship — but only the February article identifies the role DISS does play, which is confirming the eligibility that makes re-verification unnecessary. Working from the January table alone would exclude DISS from the process altogether.

• A first application is defined by the eligibility outcome. An applicant who applied elsewhere without receiving eligibility is treated as a first application at your facility.

• The rule accepts four kinds of registrar seal, not two. §117.10(c)(1)(i) reads “raised, embossed, impressed, or multicolored”. A certificate bearing an impressed or multicolored seal is acceptable, and rejecting it is an error in the contractor’s favour that delays the application. Passports must also be undamaged as well as unaltered.

Guidance changed in the preceding year

Date	Level	Source	Direction and effect	Status / basis
2026-01-01	VOI	VOI Jan 2026	Stated that verification must be conducted strictly in person, and identified email, video technology and other remote methods as not authorised.	rescinded; INFERRED - The July 2026 issue states that this guidance was incorrect and should be disregarded. Procedures written to require in-person verification on that basis should be revised.
2026-01-01	VOI	VOI Jan 2026	Listed DISS in a table of documents and systems headed Acceptable Proof for PCL Applicants? against the answer No, stating without qualification that DISS is an internal government database and cannot be used as an official source to validate U.S. citizenship for security clearance applicants.	superseded; INFERRED - The February 2026 issue limited the statement to first applications, and identified DISS as the place where current or previous eligibility is confirmed — the fact that establishes re-verification is not required. Read narrowly this is a qualification and an added role rather than a reversal: neither issue treats a DISS record as proof of citizenship. An FSO working from the January table alone would nonetheless exclude DISS from the process entirely.
2026-01-01	VOI	VOI Jan 2026	Provided that where operational needs prevent in-person verification, a trusted third party such as a notary, outside counsel or other government representative may be authorised, subject to written company procedures.	active; No supersession conclusion
2026-02-27	VOI	VOI Feb 2026	Verification is required in support of an individual's first Moderate Tier (T3) or High Tier (T4, T5) application, before DCSA begins the investigation. Re-verification is not required for subsequent applications once eligibility has been granted — for example a Continuous Vetting eligibility upgrade, or new eligibility after a break in employment. Whether an application is a first application turns on whether eligibility was granted. Where a prior application did not result in eligibility, a subsequent application — including at a new company — is treated as a first application. Re-verification before a subsequent application or before granting access remains permitted but not required. You may also ask a returning employee whether their citizenship status has changed.	active; No supersession conclusion
2026-07	VOI	VOI Jul 2026	Evidence may be examined by physical inspection, digital review, or another contractor-managed method. Record in your written procedures which method you use.	active; No supersession conclusion

Reviewer note: The July 2026 update addresses the method of examination. It states that it does not alter the list of authorised documents, and §117.10(c) continues to require originals or certified copies.Document acceptability is governed by §117.10(c)(1) and (2). Industrial Security Letters that previously added conditions were rescinded in December 2025 and are not among the four DCSA currently publishes, so no additional condition applies from that source.Three issues in seven months addressed this requirement, each qualifying the last: January set out the document exclusions and an in-person method requirement; February limited the DISS exclusion to first applications and established the one-time rule; July withdrew the in-person requirement. A procedure written from any single issue will be incomplete.

4. Current-cycle operational notices outside the Part 117 requirement catalog

These approved notices affect FSO operations but are not presented as Part 117 requirements. Their source role and operational basis remain distinct.

Topic	Detected or announced in	Operational basis	Use control
FOCI Expansion vetting for covered DoW contracts over $5M	VOI October 2026 (2026-10-30)	Section 847, Pub. L. 116-92; DoDI 5205.87; VOI October 2026	Operational notice; do not present as a CFR requirement.
National Industrial Security System Increment 2 (NI2)	VOI October 2026 (2026-10-30)	VOI October 2026	Operational notice; do not present as a CFR requirement.

5. Active ISL source-scope control

Only the four ISLs in the active source folder are carried into this edition. Archived ISLs are excluded.

Active ISL	Topics in this catalog	Use control
ISL 2021-02	Reporting Requirements and SEAD 3 Reportable Activities	Apply only within its stated scope; later applicable active guidance is paramount for execution.
ISL 2024-01	Information System Security and Commercial Cloud Services	Apply only within its stated scope; later applicable active guidance is paramount for execution.
ISL 2024-02	Submission of the SF 86 (NBIS eApp)	Apply only within its stated scope; later applicable active guidance is paramount for execution.
ISL 2026-01	Insider Threat Program and ITPSO Appointment	Apply only within its stated scope; later applicable active guidance is paramount for execution.

6. Status and recency decision controls

Review question	If yes	If no
Does the source quote text expressly withdrawing an earlier instruction?	EXPLICIT may be used; record the quotation and source.	Do not use EXPLICIT. Continue the status review.
Does a later touch address the same people, system, event, and time period?	Treat the newer applicable active touch as the execution endpoint.	Preserve both instructions within their separate scopes.
Is an earlier touch displaced only by comparison and reasoning?	Mark INFERRED and show that reasoning.	Do not imply supersession or withdrawal.
Is the subject anchored to Part 117?	State the CFR baseline before interpretation and execution guidance.	Label the topic extra-regulatory.
Does guidance conflict with the regulation or remain silent on a material fact?	Escalate; do not amend Part 117 or infer permission, prohibition, or withdrawal from silence.	Apply the stated instruction within its scope.