FSO Guidance Watch

Authority-first, chronology-aware FSO reference

DCSA interpretive and operational guidance measured against 32 CFR Part 117

Document control	Value
Edition	Draft 0.2
Current through	30 October 2026
VOI cycle coverage	January through October 2026, with an explicit disposition for every monthly issue.
Reverification	Check the linked official sources before relying on this draft after a new DCSA, ODNI, ISOO, or eCFR publication.
Distribution	Unclassified working reference; preserve source-document markings and handling requirements.
Corrections	Submit corrections to the FSO Guidance Watch maintainer.

Start here — by task

This is not the contents list restated — it groups sections by the situation you're actually in, which often spans more than one section below. Every section still gives the full CFR baseline, current DCSA direction, and guidance chronology.

If you are...	Go to
Bringing on a new employee who needs access to classified information	3.9 Verification of U.S. Citizenship · 3.8 SF 86 (NBIS eApp) · 3.2 Fingerprint Collection · 3.1 SF 312 / NDA
An employee won't sign something, is leaving, or their status just changed	3.1 SF 312 / NDA · 3.7 Reporting Requirements / SEAD 3
Something just happened that you need to report — adverse information, a foreign contact/travel, a loss or compromise, a cyber incident, or an entity/facility change	3.7 Reporting Requirements / SEAD 3 · Appendix A (full reporting matrix)
An employee's periodic reinvestigation, continuous vetting, or 5-year PVQ update is coming due	3.6 Reinvestigation and Continuous Vetting
Standing up, changing, or self-inspecting storage areas, containers, classified systems, commercial cloud, or mobile devices	3.5 Open Storage Areas · 3.3 Information System Security
Appointing, documenting, or running your Insider Threat Program	3.4 Insider Threat Program

1. Scope and use

This handbook states the Part 117 baseline first, then shows what incorporated authority and DCSA direction add. It covers the nine selected practices listed below because they have approved, operationally material source chains in this edition. It is not a complete index to Part 117, and the absence of a topic does not mean that no rule or guidance applies.

1.1 Contents

- 3.1 Classified Information Nondisclosure Agreement (SF 312) - § 117.10(g)
- 3.2 Fingerprint Collection - § 117.10(e)
- 3.3 Information System Security and Commercial Cloud Services - § 117.18
- 3.4 Insider Threat Program and ITPSO Appointment - § 117.7(b)(4)
- 3.5 Open Storage Areas (formerly Closed Areas) - § 117.15(c)
- 3.6 Reinvestigation and Continuous Vetting - § 117.10(b)(5)
- 3.7 Reporting Requirements or SEAD 3 Reportable Activities - § 117.8
- 3.8 Submission of the SF 86 (NBIS eApp) - § 117.10(d)
- 3.9 Verification of U.S. Citizenship - § 117.10(c)
- Appendix A - Detailed § 117.8 and SEAD 3 reporting matrix

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 chronology - when direction changed within the preceding year, show the current direction, every change in that window, and the immediately preceding direction when needed for context.

Section 3.7 uses a compact operational summary and routes the complete paragraph-level matrix to Appendix A because the 38-row reporting chain is too dense for the standard profile. Section 3.5 includes a separate supporting-authority update because ISOO, rather than DCSA, replaced the controlling equipment notices.

1.3 Interpretive standard

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

• Industrial Security Letters - binding DCSA supplementary procedures. DCSA issues ISLs within its cognizance. DoDI 5220.31, section 2.2(d) states: "The industrial security letters provide clarification, interpretation, and guidance to cleared companies and GCAs in carrying out their responsibilities under the NISP."

• 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 Status, recency, and conflict rules

• EXPLICIT means the cited source expressly withdraws, rescinds, replaces, corrects, reverses, or supersedes identified earlier material. The named scope limits the conclusion.

• INFERRED means the cataloger concluded that later direction overtook earlier direction, but the source did not expressly say so. Treat the reasoning as a review conclusion, not as DCSA's quoted position.

• A newer source controls only the people, systems, dates, and situations it addresses. Silence is neither permission nor prohibition.

• If direction changed within the preceding year, show the current direction and the material chronology. If it did not change, omit old history.

• When sources conflict, identify the higher authority and preserve the more protective controlling requirement until an authoritative source resolves the issue.

1.6 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

2. Sources and coverage

The catalog includes only approved findings and their recorded Part 117 anchors. Every topic below identifies whether its practice rests on rule text, incorporated authority, or DCSA guidance.

2.1 Authority coverage

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

• Fingerprint Collection - § 117.10(e)

• Information System Security and Commercial Cloud Services - § 117.18

• Insider Threat Program and ITPSO Appointment - § 117.7(b)(4)

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

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

• Reporting Requirements or SEAD 3 Reportable Activities - § 117.8

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

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

3. Requirements

3.1 § 117.10(g) - Classified Information Nondisclosure Agreement (SF 312)

Current operational direction: Execute the SF 312 before access; accept authorized ECA PKI digital signatures; omit the witness signature when the subject signs with an authorized digital signature; when a witness is used, permit remote video witnessing only by an authorized contractor representative or U.S. executive-branch employee; obtain the FSO acceptance signature; and upload the completed form to DISS. The CFR remains controlling.

What DCSA guidance adds to the rule

The rule establishes execution before access, witness and date requirements, forwarding to the CSA, and reporting a refusal. DCSA direction adds:

• acceptance of authorized ECA PKI digital signatures;

• no witness signature when the subject uses that authorized digital-signature method;

• remote video witnessing and a limited authorized-witness population when a witness is used;

• the FSO acceptance signature; and

• upload of the completed form to DISS.

Regulatory text - controlling authority

• § 117.10(g) - Determination of eligibility for access to classified information for contractor employees (last amended 2021-02-24)

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 authorized 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 authorized 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 authorized digital signature, before upload. A form uploaded without the acceptance signature is rejected.
5A	DCSA guidance	VOI Apr 2026	DCSA accepts an approved DoD CAC, approved ECA certificate, or other DoD-approved external PKI digital signature on the SF 312; wet signatures remain acceptable and an approved digital signature does not require a witness.
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 authorized 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 chronology

Date	Level	Source	Direction and effect	Status / basis
2020-11-01	VOI	VOI Nov 2020	Directed annotation of the execution date in the system of record and forwarding of the completed form to VROC, with upload into DISS as the preferred transmission method.	superseded; INFERRED - Overtaken by the current DISS upload and acceptance-block workflow.
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 authorizing ECA PKI digital signatures. Procedures adopted on the 2022 basis are worth revisiting.
2025-01-01	VOI	VOI Jan 2025	Authorized ECA PKI digital signatures and removed the witness-signature requirement for that signing method.	active; Current digital-signature direction.
2025-03-01	VOI	VOI Mar 2025	Directed upload of the completed SF 312 into DISS when no existing signed-date record resolves the requirement.	active; Current DISS transmission direction.
2026-01-01	VOI	VOI Jan 2026	Added remote video witnessing, limited authorized witnesses, and required the FSO acceptance signature.	active; Newest applicable witnessing and acceptance direction.
2026-04-30	VOI	VOI Apr 2026	Confirmed optional approved digital signatures for the SF 312 and stated that an approved digital signature does not require a witness; the same article also covers DD 441 and SF 328.	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.

Related entries

Related entries: Section 3.7 and Appendix A row 24 for an employee who refuses to execute the SF 312.

3.2 § 117.10(e) - Fingerprint Collection

Current operational direction: Submit prints when the request is sent to the subject. If DCSA places an individual on the facility's Phase III list, complete the DCSA-requested fingerprint submission even when another agency already enrolled that person. Source: VOI August 2026 (2026-08-31). 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.

Regulatory text - controlling authority

• § 117.10(e) - Determination of eligibility for access to classified information for contractor employees (last amended 2021-02-24)

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.

#	Basis	Source	Required action
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 enrollment 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	VOI August 2026, page 2	Work the facility-specific Phase III list to completion. Another agency's Rap Back enrollment does not satisfy a DCSA fingerprint-submission request.

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.

Guidance chronology

Date	Level	Source	Direction and effect	Status / basis
2016-02-01	VOI	VOI Feb 2016	Mandated electronic submission from 1 October 2016, with OPM rejecting hardcopy and the associated request if no electronic print arrived within 14 days.	active; No supersession conclusion
2016-12-01	VOI	VOI Dec 2016	Submit at the same time as or just before releasing the request in JPAS; confirm by checking for a closed SAC.	superseded; INFERRED - Origin of the old timing rule, repeated in substantially this form for nearly nine years.
2023-11-01	VOI	VOI Nov 2023	Restated the timing rule against eApp rather than e-QIP.	superseded; INFERRED - Same instruction, updated for the eApp cutover.
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	Submit prints when the request is sent to the subject for completion.	active; Current general submission-timing direction.
2026-03-31	VOI	VOI March 2026	Expanded Rap Back onboarding and directed mandatory employee advisements.	active; Applies to Rap Back onboarding.
2026-08-31	VOI	VOI August 2026	Added the facility-specific Phase III workflow: submit DCSA-requested fingerprints even when another agency already enrolled the individual.	active; Newest applicable Phase III direction.

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.

Related entries

Related entries: Section 3.8 for the same 120-day eApp signature-page and fingerprint-validity window.

3.3 § 117.18 - Information System Security and Commercial Cloud Services

Current operational direction: Permit government-issued NSA-approved CSfC mobile platforms at cleared contractor facilities when the applicable authorization and safeguarding requirements are satisfied. Source: VOI May 2026 (2026-05-01). 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 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 2021-02-24)

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 authorized in your ATO.
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.

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

Guidance chronology

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
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.

3.4 § 117.7(b)(4) - Insider Threat Program and ITPSO Appointment

Current operational direction: Apply ISL 2026-01 for insider-threat program minimum standards, ITPSO appointment, training, entity-family implementation, and self-inspection within its scope. Source: ISL 2026-01 (2026-05-20). 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.

Regulatory text - controlling authority

• § 117.7(b)(4) - Procedures (last amended 2021-02-24)

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 program 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 program; ITPSOs reappointed after it need proof of having completed INT122.16 prior to 1 July 2025.

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 program; 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.

Guidance chronology

Date	Level	Source	Direction and effect	Status / basis
2016-08-01	VOI	VOI Aug 2016	Set a 30 November 2016 deadline to establish a program, appoint a trained ITPSO, implement workforce training, and self-certify in writing to the assigned IS Rep.	expired; INFERRED - The original NISPOM Change 2 implementation deadline. Long expired, but it is where the program obligation began and why older facilities hold self-certification letters.
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.
2026-05-20	ISL	ISL 2026-01	Consolidated DCSA's current insider-threat minimum standards, resources, training, appointment mechanics, entity-family implementation, and self-inspection direction.	active; binding DCSA supplementary procedure within its scope

Reviewer note: ISL 2026-01 is dated 20 May 2026 and was announced in the July 2026 Voice of Industry. 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.

3.5 § 117.15(c) - Open Storage Areas (formerly Closed Areas)

Current operational direction: From 1 January 2026, request voluntary self-approval authority for eligible open storage areas when appropriate; use the current DCSA Form 147 process, redocument legacy spaces by 1 October 2027, and retain DCSA review authority. The CFR and applicable ISOO equipment standards remain controlling. Source: VOI December 2025 (effective 2026-01-01).

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, including the October 2026 operational-use restrictions and the 1 October 2028 retirement milestone.

Regulatory text - controlling authority

• § 117.15(c) - Safeguarding classified information (last amended 2021-02-24)

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 term 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.
7A	DCSA guidance	VOI Apr 2026	Before seeking approval for an open storage area, submit a written security-in-depth plan to the assigned ISR describing the covered area, layered complementary controls, and the classification level, type, size, and location of stored material; attach the approved plan and ISR approval letter to DCSA Form 147.
7B	DCSA guidance	VOI Apr 2026	Consult the current Qualified Products List before ordering security equipment so the selected cabinet, storage equipment, or weapons container is approved for its intended use.
7C	DCSA guidance	VOI Oct 2026	Use black label containers only for internal need-to-know separation inside an approved open storage area and for routine combination changes. Do not use one as primary classified storage outside an approved open storage area, and do not perform physical maintenance, structural repair, or locksmith drilling on one. De-label each and re-identify it with a "No Longer GSA Approved" marking; on mechanical failure, decommission it and replace it with a Red Label container; retire every black label container from classified operations on or before 1 October 2028.

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 term used 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.

Guidance chronology

Date	Level	Source	Direction and effect	Status / basis
2022-05-01	VOI	VOI May 2022	Introduced DCSA Form 147 and stated that contractors had no self-approval authority.	superseded; INFERRED - Later DCSA direction restored a voluntary request path effective 1 January 2026.
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.
2025-12-01	VOI	VOI Dec 2025	Confirmed that facilities may request voluntary self-approval authority effective 1 January 2026, subject to DCSA review.	active; Current self-approval direction.
2026-04-30	VOI	VOI Apr 2026	Specified the written security-in-depth plan, ISR approval, Form 147 attachment, and current Qualified Products List checks used for open-storage-area planning and approved-equipment procurement.	active; No supersession conclusion.
2026-10-30	VOI	VOI Oct 2026	Published USW(I&S) administrative guidance on black label containers: authorized and prohibited uses, mandatory re-identification, replacement on mechanical failure, and the 1 October 2028 retirement milestone.	active; No supersession conclusion. ISOO Notice 2026-06 remains the controlling equipment authority.

Reviewer note: Two independent schedules apply; neither is tied to the facility's security-review cycle.

• Legacy Form 147 spaces: Redocument any space still approved on the obsolete one-page form as an open storage area by 1 October 2027.

• Black-label equipment: Apply current ISOO Notice 2026-06. It replaced the earlier notices and is the controlling source for equipment deadlines and disposal.

August 2026 update - black-label security equipment

Authority level	Direct authority	What it contributes
Rule	32 CFR 117.15(b)-(c)	Requires approved safeguarding equipment and construction standards.
Incorporated authority	ISOO Notice 2026-06, August 31, 2026	Rescinds and replaces ISOO Notices 2022-03 and 2021-01, retains the current black-label deadlines, and consolidates disposal direction.
DCSA guidance	VOI August 2026, pages 4-5	Restates the deadline and end-of-service workflow for cleared contractors.

Resulting practice: Apply ISOO Notice 2026-06 as the current equipment authority. At end of service, remove classified material and approval labels; either mark the container for unclassified use or follow the prescribed lock disposition and recycling procedure.

Guidance chronology

Date	Source	Direction and effect
2025-09	DCSA reminder	Repeated the then-current black-label phase-out schedule.
2026-08-31	ISOO Notice 2026-06	Explicitly replaced the two older notices and consolidated current deadlines and disposal.
2026-08-31	VOI August 2026	Restated the operational procedure, but cited the notices that ISOO replaced the same day.
2026-10-30	VOI October 2026	Relayed USW(I&S) administrative guidance on how black label containers may still be used, what is prohibited, and the 1 October 2028 retirement milestone; it cited ISOO Notice 2021-01, which ISOO Notice 2026-06 replaced.

October 2026 update - black label container operational restrictions

Authority level	Direct authority	What it contributes
Rule	32 CFR 117.15(b)-(c)	Requires approved safeguarding equipment and construction standards.

Authority level	Direct authority	What it contributes
Incorporated authority	ISOO Notice 2026-06, August 31, 2026	Remains the controlling source for black label deadlines and disposal.
DCSA guidance	VOI October 2026, page 8	Relays USW(I&S) administrative guidance: black label containers may be used only for internal need-to-know separation within an approved open storage area and for routine combination-lock changes. Primary classified storage outside an approved open storage area, and any physical maintenance, structural repair, or locksmith drilling, are prohibited. Each container is de-labeled and re-identified with a "No Longer GSA Approved" marking, replaced with a Red Label container on mechanical failure, and retired from classified operations on or before 1 October 2028.

Resulting practice: Treat a black label container as separation furniture inside an approved open storage area, never as the safeguard itself. Plan replacement before the 1 October 2028 milestone; do not repair or drill one to keep it in service.

3.6 § 117.10(b)(5) - Reinvestigation and Continuous Vetting

Current operational direction: Do not initiate periodic reinvestigations; submit a PVQ every five years, timed from the DISS PVQ Date. Source: VOI May 2026 (2026-05-01). This is the newest applicable active guidance recorded for this topic; 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 2021-02-24)

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 chronology

Date	Level	Source	Direction and effect	Status / basis
2017-01-01	VOI	VOI Jan 2017	Moved Tier 5 reinvestigations to a six-year periodicity and directed industry to stop submitting T5 PRs unless directed, with narrow exceptions for SAP-designated programs.	superseded; INFERRED - The submission posture was revised in December 2017.
2017-12-01	VOI	VOI Dec 2017	Directed that FSOs resume submitting T5Rs at the six-year mark, with the six-year periodicity continuing until further notice.	superseded; INFERRED - Refined in February 2018: all T5Rs at six years, SAP caveat T5Rs at five.
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.
2026-05-01	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 continues alongside the five-year PVQ cycle; maintain the DISS record and submit the five-year update when eligibility continues without access.

3.7 § 117.8 - Reporting Requirements or SEAD 3 Reportable Activities

Current operational direction: Start with the event and the person involved, identify the controlling source, then send the report to every required destination. A DISS submission does not replace a separate FBI, DCSA CISA, DoD CSO, or ISOO report.

What the CFR requires

32 CFR Part 117.8 requires internal reporting procedures and establishes the contractor's duties for adverse information, suspicious contacts, employee-status changes, entity and facility changes, loss or compromise, certain cyber incidents, and duplicative security reviews. It incorporates SEAD 3 for covered-individual reporting but does not reproduce SEAD 3's event list.

What SEAD 3 incorporates into the rule

Population or event	Incorporated requirement
All covered individuals	Report the SEAD 3 events that apply to eligibility, conduct, foreign contacts, foreign activities, and other covered circumstances.
Unofficial foreign travel	Provide the itinerary before travel, review NCSC Safe Travels, obtain any required threat-based briefing, and report deviations or emergency travel after return.
Foreign contacts	Report contacts that meet SEAD 3's relationship, obligation, concern, or foreign-intelligence criteria; official-duty contacts and official contract travel remain subject to SEAD 3's stated exclusions.
Top Secret or Q access	Apply the additional SEAD 3 financial, foreign-property, foreign-business, voting, cohabitant, marriage, adoption, and foreign-roommate categories.

What ISL 2021-02 adds

These are Binding DCSA supplementary procedures for entities within DCSA's cognizance:

- Maintain written procedures describing how the facility receives, processes, manages, and submits covered-individual reports.
- Treat a covered individual as a person granted eligibility through the NISP, or being processed for it.
- Use DISS as the DoD-designated personnel-reporting channel; do not resubmit information already recorded on the SF 86 or in DISS.
- Send foreign-intelligence-entity contacts to both DISS and the facility's DCSA CISA, and coordinate post-travel debriefings when required.
- Apply the ISL-only cryptocurrency and psychological-health categories within the ISL's scope.

Where each report goes

Event	Required destination
Covered-individual and personnel-security reporting	DISS, unless the governing source specifies an additional destination.
Foreign-intelligence-entity contact	DISS and the facility's DCSA CISA.
Entity or facility changed condition	NISS Change Condition package; beginning 1 October 2026, Entity Vetting processes the package while the assigned ISR retains completion visibility.
Material FOCI change, or a FOCI Expansion request from Entity Vetting	NISS Change Condition package using the revised nine-question SF 328; DCSA retrieves SEC Schedule 13D and 13G filings itself and the separate Statement of Full Disclosure of Foreign Affiliations is retired (VOI Oct 2026).
Espionage, sabotage, terrorism, or subversive activity	Nearest FBI field office; promptly notify the CSA and provide it a copy of the written FBI report.

Event	Required destination
Loss, compromise, or suspected compromise	CSA through the preliminary-inquiry, initial-report, and final-report process.
Covered classified-system cyber incident	Designated DoD CSO.
Redundant or duplicative CSA review	Director, ISOO.

Detailed reference

The complete source-by-source reporting matrix is preserved in Appendix A. Use it when a specific event requires paragraph-level authority or a detailed reporting action.

3.8 § 117.10(d) - Submission of the SF 86 (NBIS eApp)

Current operational direction: Use NBIS eApp, the identified successor to e-QIP, to submit the electronic SF 86 under §117.10(d). Source: ISL 2024-02 (2024-05-01). 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 2021-02-24)

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 chronology

Date	Level	Source	Direction and effect	Status / basis
2023-04-01	VOI	VOI Apr 2023	Federal Investigations Notice 23-02 directed contractors to obtain NBIS accounts and transition applicants from e-QIP to eApp, which would replace e-QIP on 1 October.	superseded; INFERRED - The transition completed. DCSA announced full transition to eApp on 3 December 2024.
2023-09-01	VOI	VOI Sep 2023	Set out how requests initiated before 1 October would be completed in e-QIP and submitted to Vetting Risk Operations, with re-initiation in eApp only where a request was later found unacceptable or discontinued.	expired; INFERRED - A transition-window accommodation. Spent.
2023-12-01	VOI	VOI Dec 2023	Reopened the DISS Investigation Request Link so subjects could log into e-QIP and download historical SF-86 archival copies, auto-cancelling after seven days.	superseded; INFERRED - An archival retrieval path only. New background investigation requests and CV updates always went through NBIS.
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

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.

Related entries

Related entries: Section 3.2 for fingerprint timing and the shared 120-day validity window; Section 3.9 for first-application citizenship verification.

3.9 § 117.10(c) - Verification of U.S. Citizenship

Current operational direction: When operational needs prevent in-person verification, use an authorized trusted third party under written company procedures and record the verification method used. Source: VOI Jan 2026 (2026-01-01). 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 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 2021-02-24)

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.

#	Basis	Source	Required action
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 chronology

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 authorized.	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 authorized, subject to written company procedures.	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 authorized 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.

Related entries

Related entries: Section 3.8 because first Moderate Tier or High Tier application processing triggers this verification workflow.

4. Active ISL source-scope control

Active ISL	Topic in this handbook	Use control
ISL 2021-02	Reporting Requirements and SEAD 3	Covered-individual reporting, DISS submission, foreign-intelligence-entity reporting, travel coordination, cryptocurrency, and psychological-health categories for entities under DCSA cognizance.
ISL 2024-01	Information Systems and Commercial Cloud Services	DCSA verification methods for IL6 commercial cloud services and related authorization evidence within the letter's contract scope.
ISL 2024-02	Submission of the SF 86 through NBIS eApp	NBIS eApp as the successor to e-QIP for electronic SF 86 submission under § 117.10(d).
ISL 2026-01	Insider Threat Program	Insider-threat program minimum standards, ITPSO appointment, training, entity-family implementation, and self-inspection for entities under DCSA cognizance.

Appendix A - Detailed § 117.8 and SEAD 3 reporting matrix

This appendix preserves the complete approved reporting matrix. The main section is the operational entry point; this table supplies paragraph-level authority, reporting group, and detailed actions.

Appendix A.1 - Program, scope and channel

#	Authority basis	Source	Required action
1	Rule	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.
2	Binding DCSA supplementary procedures	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	VOI Jan 2025	Have that written procedure ready to produce at every scheduled security review, including remote reviews.
4	Incorporated authority	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 Incorporated authority would survive withdrawal of the ISL.
5	Binding DCSA supplementary procedures	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	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	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.

Appendix A.2 - Personnel — adverse information and conduct

#	Authority basis	Source	Required action
8	Rule	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	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	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	ISL 2021-02	Base adverse information reporting on the 13 adjudicative guidelines in SEAD 4.
12	Rule	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.

Appendix A.3 - Personnel — foreign travel, contacts and finances

#	Authority basis	Source	Required action
13	Rule	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	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.

#	Authority basis	Source	Required action
15	Incorporated authority	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	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	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.
18	Binding DCSA supplementary procedures	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	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	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.

Appendix A.4 - Employee status and eligibility events

#	Authority basis	Source	Required action
21	Rule	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	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	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	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).

Appendix A.5 - Entity and facility conditions

#	Authority basis	Source	Required action
25	Rule	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	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	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.
27A	DCSA guidance	VOI Sep 2026	Continue submitting changed-condition packages through NISS. Beginning 1 October 2026, Entity Vetting processes them, including packages for NAESOC facilities; the assigned ISR retains visibility after completion.
28	Rule	32 CFR 117.8(c)(8)	Report any change in your storage requirement or capability to safeguard classified material.
29	Rule	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	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	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	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	32 CFR 117.8(c)(13)	Report receipt of classified material from foreign interests that did not come through USG channels.

Appendix A.6 - Espionage, loss, cyber and ISOO

#	Authority basis	Source	Required action
34	Rule	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	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	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	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.
38	Binding DCSA supplementary procedures	ISL 2021-02	Stop citing ISL 2011-04 for adverse information reporting examples. This ISL cancels, incorporates and rescinds it.

Appendix B - January–October 2026 VOI source coverage

This cumulative edition contains a disposition for every DCSA Voice of Industry issue from January through October 2026. Detailed requirement sections remain controlling for the complete practice and authority chain.

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	Security-in-depth plans for open storage areas; approved equipment procurement; approved digital signatures for DD 441, SF 312 and SF 328; and DD 254 marking review before NISS upload. A classified or mismarked DD 254 must not be uploaded to NISS; secure it, initiate the appropriate inquiry, coordinate with the GCA or prime for a classification determination and corrected unclassified version, and report a security violation if classified material was placed in NISS or another unclassified contractor system.
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	National Industrial Security System Increment 2 (NI2) announcement with its FOCI Expansion, DD 254 Submission, and NISP modules; FOCI Expansion assessments for covered DoW contracts over $5 million under Section 847 of Public Law 116-92 and DoDI 5205.87, with Entity Vetting contacting facilities and an updated SF 328 required; the revised nine-question SF 328 (binding authority as a means of control; 15 percent foreign-income threshold; DCSA retrieves SEC filings); DCSA investigator title changes and the credential-only identification standard; the FY27 goal of 6,000 security reviews with the baseline review-frequency table and the FY26 results; USW(I&S) black label container operational restrictions with the 1 October 2028 retirement milestone; and continuing NAESOC rolling migrations.