INDUSTRY REPORTING

Entity Quick Reference

What your facility must report to the Government. Individual SEAD 3 reporting is on a separate sheet.

FACILITY SECURITY OFFICER	Name	Email
CSA / ISR	Name	Email

01 THE BASICS 32 CFR 117.8(a)

Who this covers	Contractors and their cleared employees, pursuant to this rule, SEAD 3, and CSA-provided guidance. This sheet covers the contractor's (entity's) own duties.
Tell your people	Establish internal procedures so employees with eligibility for access know their responsibility to report pertinent information to the FSO.
Where it goes	Report to the FBI, the CSA, or ISOO as specified in 117.8(b), (c), and (g). Provide complete information so the CSA can determine whether classified information is adequately protected.
Mark it right	Mark reports containing classified information per 117.14. Mark a report containing information submitted in confidence as such.
Privacy Act	Reports about an individual may withhold certain information under 5 U.S.C. 552a, including a source's identity where confidentiality was promised.

02 REPORT TO THE FBI 32 CFR 117.8(b)

Espionage, sabotage, terrorism, subversion	Promptly submit a written report to the nearest FBI field office on actual, probable, or possible activity at any of your locations. An initial report may be by phone but must be followed up in writing regardless of the FBI's disposition.
Tell the CSA too	Promptly notify the CSA when you report to the FBI, and give the CSA a copy of the written report.

03 REPORT TO THE CSA: YOUR PEOPLE 32 CFR 117.8(c)(1)-(6)

Adverse information	Report adverse information concerning any employee eligible for access. No rumor or innuendo. Termination of employment does not negate the requirement; if 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.
Suspicious contacts	Efforts by anyone, regardless of nationality, to obtain illegal or unauthorized access to classified information, or to elicit information from an eligible employee, or any contact suggesting the employee may be targeted by a foreign intelligence service. See SEAD 3 for the specific information to report.
Employee status changes	Death · change in name · termination of employment · change in citizenship. Report by the CSA-designated reporting mechanism.
Naturalization	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.
Won't process or won't continue	Report when an employee no longer wishes to be processed for eligibility, or to continue having access, and the reason for the request.
NDA refusal	Report an employee's refusal to sign the SF 312 or other approved NDA.

Becker v. Philco, 372 F.2d 771 (4th Cir. 1967), cert. denied 389 U.S. 979 (1967): a contractor is not liable for defamation over communications required of it under this rule or a classified contract.

WHEN IN DOUBT, REPORT IT. These are the entity's own duties to the Government, separate from what your people report about themselves under SEAD 3. A report under 117.8 does not excuse an individual reporting duty, and an individual report does not excuse yours.

Sources: 32 CFR Part 117.8(a), (b), (c). This sheet summarizes published policy and does not supersede it. Individual/personal reporting under SEAD 3 is on a separate sheet. Pages 2-3: entity conditions, loss/compromise, culpability, cyber, and ISOO reports. Questions go to your CSA/ISR. Current as of October 2026.

Industry Reporting — Entity and Facility Conditions

04 REPORT TO THE CSA: YOUR ENTITY 32 CFR 117.8(c)(7)-(14)

Changed conditions	Submit covered ownership/control, operating name/address, KMP, business termination or reorganization, and material FOCI changes through a NISS Change Condition package. Beginning 1 October 2026, Entity Vetting processes the package, including for NAESOC facilities; the assigned ISR retains completion visibility.
Name or address change	Change of operating name or address of the entity or any location eligible for access to classified information.
KMP changes	Any change to previously submitted KMP information. State whether new KMP are cleared and at what level, excluded under 117.7(b)(5)(ii), or temporarily excluded under 117.9(g).
Ending the business	Any action to terminate business or operations, imminent bankruptcy or reorganization, or any change that might affect the validity of your eligibility.
FOCI change	Any material change to previously reported foreign ownership, control, or influence. Submit an updated SF 328; do not repeat unchanged answers. Report discussions or agreements that could reasonably lead to foreign control in writing, and forward any Schedule 13D received.
Storage capability change	Report any change in your storage requirement or capability to safeguard classified material.
Can't safeguard right now	Report any emergency situation that renders your location incapable of safeguarding classified material as soon as possible.
Prime/sub problems	Prime contractors report anything indicating a subcontractor cannot adequately protect classified information or that affects the validity of a subcontractor's eligibility. Subcontractors report the same about their prime, and notify their prime whenever they make a (c)(7)-(10) report.
Recovered material	Report when the location or disposition of material previously terminated from accountability is later discovered and brought back into accountability.
Foreign classified contracts	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.
Improper foreign material	Report receipt of classified material from a foreign interest that did not come through USG channels.

05 LOSS OR COMPROMISE 32 CFR 117.8(d)

Preliminary inquiry	Immediately upon a security violation report, initiate a preliminary inquiry into all circumstances of the presumed loss, compromise, or suspected compromise, including validating the classification.
Initial report	If the preliminary inquiry confirms an incident, promptly submit an initial report unless the CSA notifies you otherwise.
Final report	On completion, submit a final report: new material facts, the responsible individual's full name and SSN and any prior incident record, corrective action taken, disciplinary action taken, and the specific reasons for the conclusion reached.

Sources: 32 CFR Part 117.8(c)(7)-(14) and (d); VOI September 2026. This sheet summarizes published policy and does not supersede it. Questions go to your CSA/ISR. Current as of October 2026.

Industry Reporting — Culpability, Cyber, and ISOO

06 CULPABILITY REPORTS 32 CFR 117.8(e)

Track it	Establish a system to manage and track employees who violate this rule, so you can identify patterns of negligence, carelessness, or a potential insider threat.
Graduated response	Establish and apply a graduated scale of administrative and disciplinary action for violations or negligence. Submit a final report to the CSA with the culpability findings and corrective actions taken.
State the factor	When the responsible individual can be identified, state whether the violation involved deliberate disregard, negligence in handling classified material, or a recent/recurring pattern of questionable judgment, irresponsibility, negligence, or carelessness.

07 CDC CYBER INCIDENT REPORTS 32 CFR 117.8(f) — CDCs only

Report immediately	Cleared Defense Contractors: immediately report to the designated DoD CSO any cyber incident on a classified covered information system that CSO has approved. Include the technique used, a sample of any isolated malicious software, and a summary of any DoD program potentially compromised.
Non-Federal systems	Report cyber incidents on non-Federal, unclassified information systems in accordance with your contract requirements.
Give DoD access	Allow DoD personnel access, on request, to equipment and information needed to conduct forensic analysis of a reportable cyber incident.

08 REPORTS TO ISOO 32 CFR 117.8(g)

Duplicative review	Report instances of redundant or duplicative security review or audit activity by CSAs to the Director, ISOO, for resolution.
Duplicate processing	Report instances of a CSA duplicating processing of an entity eligibility determination that another CSA has already made.

THIS SHEET IS THE ENTITY'S DUTY, NOT YOUR PEOPLE'S. 32 CFR 117.8(a) applies to contractors and their cleared employees together; (b) through (g) are the contractor's own reporting duties to the Government. What an individual must report about themselves is SEAD 3, on the Clearance Holder sheet — not this one.

Source: 32 CFR Part 117.8(e), (f), (g). CDC cyber incident reporting (f) applies only to Cleared Defense Contractors, pursuant to 10 U.S.C. 391 and 393 and DFARS 252.204-7012. This sheet summarizes published policy and does not supersede it. Questions go to your CSA/ISR. Current as of October 2026.