AVALON

TECHNICAL BRIEF · BASED ON GAO-26-108606 · DOW, GOVERNMENT-WIDE

GAO COUNTED SEVEN CYBER REPORTING REQUIREMENTS ACROSS FIVE DIB RULES

80 of 117

FEDERAL CYBER REGULATIONS CARRY REPORTING REQUIREMENTS GAO FLAGGED AS POTENTIALLY DUPLICATIVE; FIVE OF THE 117 REACH THE DIB

GAO's July 2026 review of 117 federal cyber regulations lists five that reach the defense industrial base. Its tables show three take incident reports, two take plans, and two take assessments, with the DFARS clauses in all three. GAO made no recommendations.

THE FINDING

In July 2026, GAO published Cybersecurity Regulations: Multiple Sectors Are Subject to Potentially Duplicative Reporting Requirements (GAO-26-108606). It identified 117 cyber regulations from 37 federal agencies, spanning nine critical infrastructure sectors. Of the 117, 80 (about 70 percent) carry reporting requirements GAO flagged as potentially duplicative, at least 125 requirements in all.

GAO defined the test by type. Regulations that ask for the same kind of reporting, especially within one sector or across several, have the potential to be duplicative or conflicting.

The defense industrial base (DIB) is one of the nine sectors, and Table 3 lists five regulations for it: 32 CFR Part 117, 32 CFR Part 170, 32 CFR Part 236, 48 CFR Part 252, and 32 CFR Part 2004. Counting GAO's yes marks, Avalon tallies seven requirements across the five. GAO does not name any DIB rule as duplicating a specific counterpart, and it made no recommendations.

GAO TABLE 3 REGULATION	INCIDENTS	PLANS, TECHNICAL DATA	REVIEWS, ASSESSMENTS
32 CFR Part 117 (NISPOM)	Yes	Yes	No
32 CFR Part 170 (CMMC Program rule)	No	No	Yes
32 CFR Part 236 (DIB cybersecurity activities program)	Yes	No	No
48 CFR Part 252 (contract clauses, incl. DFARS)	Yes	Yes	Yes
32 CFR Part 2004 (NISP)	No	No	No

WHY IT KEEPS HAPPENING

GAO's account of the fix is mostly an account of a pause. The Office of the National Cyber Director (ONCD) is responsible for coordinating the streamlining of regulations, and National Security Memorandum-22 (NSM-22) says the National Cyber Director should coordinate with agencies on harmonization.

After Executive Order 14239 in March 2025, CISA officials told GAO, the executive branch paused activities under that memorandum, including harmonization efforts. GAO reported the review still underway as of June 2026. As of July 2026, the administration had not released implementation plans for its strategy, and GAO said those plans could help clarify lead agency roles.

Contract text adds its own churn. GAO flagged that the FAR was under substantial revision as of June 2026, so Title 48 citations, including the DFARS row above, may change.

WHY IT MATTERS TO YOUR BID

The DFARS row is the one a DoW (formerly DoD) capture manager already carries, and the only DIB regulation in GAO's table that takes incident reports, plans, and assessments. Which of the other four apply to a given contractor, the table does not say.

A technical volume shows how a team handles that. Evaluators reading for understanding of the requirement look for a team that knows which document answers which request, and for subcontract terms that flow down the right obligations. A volume that rewrites the system description for each ask, or cites clause numbers that a rewrite may move, shows risk.

Avalon has also written about what industry panelists told GAO.

TECHNICAL APPROACH

The method below comes from Avalon's System and Application Security Plans service, and it describes how the work is done. A contractor handling CUI needs its own plan under NIST SP 800-171 requirement 3.12.4 in Revision 2, numbered 03.15.02 in Revision 3.

1. **Validate the boundary and categorization.** Confirm which systems and data each rule reaches, and write the boundary, the FIPS 199 impact level, and the information types into one worksheet. Work on classified systems under 32 CFR Part 117 sits outside this method, which is unclassified.

2. **Characterize the system once.** Produce network and data-flow diagrams, a component inventory reconciled to what is deployed, ports and services, and interconnections. These are the plans and technical information every request asks for, so they are written once and cited.
3. **Build the control implementation workbook.** For each requirement, record the status (implemented, partially implemented, planned, inherited, or not applicable), a system-specific narrative, and an evidence pointer. The same pointers answer a review, an audit, or a self-assessment request. Deficiencies found while drafting go to a gap log formatted for POA&M intake.
4. **Write the incident reporting narratives from the same record.** For the incident response and reporting requirements, each narrative states who reports, through what mechanism, and where the evidence lives, including the DFARS 252.204-7012 report due within 72 hours of discovery. The plan points to the incident response plan as a companion document; writing that plan is separate, priced work.
5. **Run assessor-lens QA and write the maintenance guidance.** A reviewer reads each narrative the way a control assessor will, and a two to three page procedure keeps the plan current under continuous monitoring.

Avalon is not a CMMC C3PAO, does not conduct or replace the independent assessment, and does not decide which rule governs. The contractor submits its own reports.

WHAT "FIXED" LOOKS LIKE

GAO made no recommendations, so it has no closure evidence to cite. For a contractor, these are targets:

- One system security plan that answers each DIB request, with the section named and no fact written twice.
- Incident reporting narratives that match what the contract requires and name their evidence.
- A maintenance procedure that names who updates the plan when a clause changes.

STATUS CHECK

OPEN GAO-26-108606 contains no recommendations, so no status exists to track.

TEAMING FIT

NAICS	541512, 541519
AVALON'S SUB ROLE	Contractor-side system security plan and characterization, control workbook with evidence pointers, POA&M gap log, assessor-lens QA, and maintenance guidance, under the prime's compliance task
SMALL-BUSINESS STATUS	Small business; HUBZone (in progress)
LIKELY VEHICLES	GSA MAS (SIN 54151HACS Highly Adaptive Cybersecurity Services); GSA MAS (SIN 54151S IT Professional Services); GSA OASIS+

If DoW work with covered defense information is in your capture plan, Avalon teams as the sub that builds the one security plan every DIB request draws from.

BRANDON IRELAND, FOUNDER · CONTACT@AVALONTECHSERVICES.COM · AVALONTECHSERVICES.COM

This brief analyzes publicly released oversight reports. It does not describe work Avalon performed for any agency named.