AVALON

TECHNICAL BRIEF · BASED ON GAO-26-107955 · DOW

CMMC ASSESSMENT CAPACITY: WHAT GAO FLAGGED BEFORE THE PHASE 2 PAUSE

4 months

BETWEEN GAO'S MARCH 2026 REPORT ON CMMC EXTERNAL FACTORS AND DOW'S JULY 2026 PHASE 2 SUSPENSION

In March 2026, GAO found DoD had not assessed how it would handle the risk that private-sector assessors couldn't meet CMMC demand. In July, DoW suspended Phase 2 and its third-party assessments. GAO's recommendation is open, and the contract requirements under DFARS 252.204-7012 never paused.

THE FINDING

On March 12, 2026, GAO published Defense Contractor Cybersecurity: DOD Should Address External Factors That Could Impede Program Implementation (GAO-26-107955). It reviewed DoW (formerly DoD) plans for the Cybersecurity Maturity Model Certification program, which DoD set up in 2020 and planned to implement over three years.

GAO found that DoD had only partially addressed the external factors that could keep the program from meeting its goals. Specifically, DoD had not assessed and documented how it intended to mitigate the risk that private-sector capacity would be insufficient to meet its needs for assessments. DoD officials told GAO that leaders could issue waivers if outside factors caused significant problems; GAO noted that waivers would not address the underlying challenges.

GAO recommended that the DoD CIO assess and document the key external factors and develop approaches to address them. DoD concurred.

WHY IT KEEPS HAPPENING

CMMC depends on assessors DoW doesn't employ. Level 2 certification relies on accredited third-party assessment organizations, and their capacity is set by the market, not by the program's schedule. GAO also found that DoD had no single strategic plan for the program, only several planning documents.

The sequence since the report is a matter of record. On April 29, 2026, DoD submitted a corrective action plan saying it would document results by December 31, 2026.

Then, on July 13, 2026, a DoW CIO memorandum, a non-GAO source, suspended the planned November 2026 move to Phase 2. Program managers may not designate CMMC Level 2 third-party or Level 3 assessments during the review, no waivers will be granted, and only Level 1 and Level 2 self-assessments are allowed. The memo says further guidance will follow the CIO's 60-day review.

GAO's report didn't cause the suspension, and this brief doesn't claim it did. The two describe the same constraint: assessments need assessors.

WHY IT MATTERS TO YOUR BID

The memo is explicit on one point: the cybersecurity requirements in DFARS 252.204-7012 remain in effect. That clause carries NIST SP 800-171. Under requirement 3.12.4 of SP 800-171 Rev. 2, a contractor must develop, document, and periodically update a system security plan for the nonfederal systems that handle controlled unclassified information, describing the boundary, the environment, and how each requirement is met.

What paused is the third-party check, not the obligation.

For a prime, that cuts two ways. Its own CUI environment still needs a plan that would survive an assessor reading it. Its suppliers do too, and a supplier whose SSP is template language is a risk the prime carries into every DoW program.

Timing is the second issue. If third-party assessments resume, the companies that waited will compete for the same limited assessor capacity GAO flagged. CMMC carries the same SSP requirement as a Level 2 practice, CA.L2-3.12.4, so a plan that is accurate now is work that won't be waiting when the queue forms.

TECHNICAL APPROACH

The method below comes from Avalon's System Security Plans service, applied to a contractor's CUI environment under SP 800-171 Rev. 2. It describes how the work is done, at the methodology level, and runs inside the prime's own environment.

1. **Validate the boundary before writing anything.** Confirm where CUI is stored, processed, and transmitted, and draw the boundary around those systems. A boundary drawn too wide inflates the plan; one drawn too narrow leaves CUI outside it. Flag questionable scoping decisions before they spread through every section.
2. **Characterize the environment.** Reconcile the hardware and software inventory, document network and data-flow diagrams, user types and privileges, and interconnections. Where a cloud provider supplies controls, verify the inheritance against that provider's customer responsibility matrix rather than assuming it.
3. **Write each implementation statement for this environment.** For every requirement, state who performs it, what mechanism enforces it, and where the evidence lives, with an accurate status: implemented, partially implemented, planned, inherited, or not applicable. "Planned" is an acceptable answer; a falsely clean plan is not.
4. **Log the gaps for POA&M intake.** Every deficiency surfaced while drafting goes into a gap log formatted for direct entry into the plan of action, so self-assessment scores and remediation plans start from the same list.
5. **Read it like an assessor, then keep it current.** Run an assessor-lens QA pass that reads each narrative the way an assessment team will, walk it through with the system owners, and leave short maintenance guidance so the plan tracks the environment as it changes.

Avalon writes plans; it does not assess them. Avalon is not a third-party assessment organization and does not certify CMMC compliance or guarantee an assessment outcome.

WHAT "FIXED" LOOKS LIKE

For GAO's recommendation, closure means DoD documents the key external factors, including assessor capacity, and the approaches it will take to address them. Its corrective action plan targets December 31, 2026.

For a prime and its suppliers, the targets are practical:

- A current SSP for each CUI environment, with accurate implementation status on every requirement.
- A gap log that matches the plan of action and the self-assessment score.
- Inherited controls verified against the provider's documentation.

STATUS CHECK

OPEN The recommendation was open as of GAO's last update, which records DoD's April 29, 2026 corrective action plan. DoW's Phase 2 suspension took effect July 13, 2026, pending the CIO's review.

TEAMING FIT

NAICS	541512, 541690
AVALON'S SUB ROLE	SP 800-171 system security plan development for the CUI environments in the prime's DoW program: boundary validation, system characterization, implementation statements, and a gap log ready for POA&M intake
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 program work that touches CUI is in your capture plan, Avalon teams as the sub that writes the system security plans your environment and your suppliers will need, whatever the next CMMC assessment model looks like.

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.