CYBER SECURITY SOLUTIONS

CLIENT ADVISORY
securedbycss.com · ISSUED 7/14/2026
RE: CMMC PHASE II SUSPENSION

CMMC Phase II is suspended. Your obligations are not.

A plain-language briefing on the July 13, 2026 Department of War memorandum — what changed, what did not, and what it means for your compliance program right now.

SOURCE: dodcio.defense.gov/CMMC **EFFECTIVE:** Jul 13, 2026 **STATUS:** Program paused in Phase 1

On July 13, 2026, the Department of War announced the **immediate suspension of CMMC Phase II** — the transition, scheduled for November 10, 2026, that would have made third-party certification assessments a condition of award on applicable contracts. A 60-day reform task force and an industry RFI are now underway. This is a real development, but it is far narrower than the headlines suggest. The Department was explicit: this is **not** a rollback of cybersecurity expectations. Your duty to implement, self-assess, and truthfully report your compliance is unchanged. The Department framed the pause as part of an effort to speed acquisition and lower barriers for small and non-traditional businesses — a change to **how compliance is verified**, not a repeal of the requirement to be secure.

COMPLIANCE STATUS — AT A GLANCE

● STILL IN EFFECT

Binding today — no change

- ✓ **DFARS 252.204-7012** — safeguard Covered Defense Information; report cyber incidents.
- ✓ **NIST SP 800-171 Rev 2** — all 110 security requirements still apply.
- ✓ **Phase 1 self-assessments** — Level 1 (Self) & Level 2 (Self) still required.
- ✓ **SPRS score + annual affirmation** — remain live representations to the Government.
- ✓ **Select government-led assessments** — the Department will still verify.

● ON HOLD

Suspended pending 60-day review

- **The Nov 10, 2026 move to Phase II** is suspended until further notice.
- **Third-party C3PAO (Level 2)** assessments may no longer be a condition of award.
- **DIBCAC (Level 3)** certification designations are likewise paused.
- **Program's long-term shape** is under CMMC Reform Task Force review + RFI.

THE ONE THING TO UNDERSTAND

What paused is the outside audit — not the work.

CMMC never created new security requirements. It added a mechanism to **verify** the controls you already owe under DFARS and NIST 800-171. Suspending Phase II pauses **who checks your homework** — it does not pause the homework, your self-assessment, or your obligation to report it accurately. Every control you owed on July 12 you still owe today.

ⓘ How we got here

CMMC was built through two rulemakings. **32 CFR Part 170** established the program's architecture, assessment levels, and oversight structure and took effect **December 16, 2024**. **48 CFR** folded CMMC into the acquisition process and took effect **November 10, 2025**, starting the phased rollout. Phase 1 made a **self-assessment** a condition of award for new solicitations and opened SPRS for score submissions. Phase 2 — the part now suspended — would have required an independent **C3PAO audit** before award on CUI contracts.

CMMC 2.0 TIMELINE

WHAT CHANGED ON 7/13 — AND WHAT THE FAR CUI RULE ADDS

SCOPE	ORIGINAL DOW CMMC (CUI)	DOW CIO UPDATE — 7/13/2026	PROPOSED FAR CUI RULE
Phase 1 timeline	Nov 10, 2025 – Nov 9, 2026	Nov 10, 2025 – Nov 9, 2026	**No phased role; expected Q4 2026**
Phase 2 timeline	Nov 10, 2026 – Nov 9, 2027	**TBD — after 60-day review (Phase 1 extended)**	N/A
DFARS 252.204-7021 (CMMC)	Active	Active	N/A
Supply-chain flow-down	Yes	Yes	Yes
Self-attestation requirement	Yes — L2 / NIST 800-171 Rev 2	Yes — L2 / NIST 800-171 Rev 2	**Per agency / NIST 800-171 Rev 3**
L2 C3PAO / 800-171 cert.	At DoW discretion	**Delayed pending program review**	**Per agency / Rev 3**
L3 DIBCAC / 800-172 cert.	Under Phase 2 (DoW discretion)	**Delayed pending program review**	**Per agency / NIST 800-172**
Incident reporting (7012)	72 hours	72 hours	72 hours
Cloud for CUI	FedRAMP Moderate or DoD-memo equiv.	FedRAMP Moderate or DoD-memo equiv.	FedRAMP Moderate baseline

Comparison of regulatory status across the original CMMC schedule, the 7/13/2026 DoW CIO update, and the proposed FAR CUI rule (FAR Case 2026-001). Framework adapted from public analysis by Summit 7.

01 Your existing contracts still bind you

If you hold DoD/DoW contracts containing the DFARS 252.204-7012, -7019, and -7020 clauses — as effectively every contract involving CUI does — you have **already** implemented (or committed to implement) the 110 NIST 800-171 controls, posted a self-assessment score to **SPRS**, and affirmed compliance through a senior company official. Those representations are in force **today**. Nothing in the memo relieves you of them, and Level 2 (Self) still requires a self-assessment every three years with an **annual affirmation** — an affirmation that lapses, and takes your status with it, if you fail to renew it. The same safeguarding obligations **flow down to your subcontractors**, so gaps anywhere in your supply chain remain your exposure. And that affirmation is a **personal attestation by a named senior official** — not a routine staff box-check. None of that changed on July 13.

Two practical wrinkles: existing solicitations and contracts that already carry a Level 2 (C3PAO) or Level 3 (DIBCAC) requirement are being **amended to remove it**, and DoW is cleaning up active solicitations now. But if you are a **prime**, that removal doesn't erase your DFARS duties; and if you are a **subcontractor**, your prime may still contractually require a third-party assessment as a condition of doing business. Confirm your specific obligations with your Contracting Officer (KO) or prime — don't assume the pause changed your contract.

02 The suspension raises your False Claims Act exposure

LEGAL RISK — READ CAREFULLY

Pausing third-party audits does not lower your legal risk — it **concentrates** it. With outside assessors out of the loop, the Government is relying more heavily on what you **self-certify**. When a company knowingly posts an inflated SPRS score, affirms compliance it has not achieved, or invoices a contract while materially misrepresenting its cybersecurity posture, it can face liability under the federal **False Claims Act (FCA)**.

- DOJ's **Civil Cyber-Fraud Initiative** pursues these cases and enforcement is ongoing — in June 2026, DOJ settled with a contractor for **$507,144** after it self-reported a perfect SPRS score of 110 that a later DIBCAC assessment scored at **-170**.
- FCA claims can be filed by the Government **or by whistleblowers** — often your own employees — who share in the recovery.
- Exposure includes **treble (3×) damages** plus per-claim penalties.

Liability turns on **knowledge** — a company that knew, or recklessly disregarded, that its representation was false. Honest gaps you are actively documenting and remediating are a fundamentally different posture from a score you cannot support.

The safest position never changed: do the work, document it, and certify only what is true.

03 The 180-day POA&M clock is still running

180
DAYS
to close out a Level 2 (Self) POA&M

Even in a self-assessment-only world, the rules on gaps are unchanged. A Level 2 (Self) contractor that scores well enough to earn **Conditional** status may carry limited unmet items on a Plan of Action & Milestones (POA&M) — but under 32 CFR 170.21 those items **must be closed within 180 days** of the Conditional status date, confirmed by a closeout self-assessment. Miss the window and Conditional status expires, with standard contractual remedies. (Level 1 allows no POA&M at all.) Knowing where you stand, and remediating on the clock, is a **present-day** requirement — not a future one. That makes an accurate, current self-assessment score more valuable than ever: it is at once your contractual representation to the Government and your first line of defense if your posture is ever questioned.

04 Assessments haven't stopped

C3PAOs remain **fully authorized** to conduct assessments and issue certifications, and results can still be uploaded to eMASS. If you already have a C3PAO assessment on the calendar, you have two defensible paths:

PATH A · PROCEED

Complete the assessment

Go ahead and certify. A finished CMMC certification is a genuine market differentiator and hard proof of your ability to protect CUI — and it puts you ahead of the field when the requirement returns.

PATH B · PAUSE

Hold and watch the review

Wait to see how the 60-day review resolves before scheduling. There's no penalty for pausing — provided you keep meeting your DFARS and self-assessment obligations in the meantime.

Either way, DCMA **DIBCAC assessments continue** under DFARS 252.204-7019/-7020, which are independent of the CMMC rule — so a current, accurate SPRS score stays mandatory regardless of which path you choose.

05 A bigger rule is coming — and the pause doesn't touch it

Separately from CMMC, the FAR Council's proposed **FAR CUI rule (FAR Case 2026-001)**, republished June 23, 2026 under the Revolutionary FAR Overhaul, would extend CUI protection to **all civilian federal contracts** — not just DoD. If you hold civilian agency work alongside your defense contracts, a single 800-171 program can cover both. Its key terms:

LIVES IN **FAR Part 40**	SECURITY BASELINE **NIST 800-171 Rev 3**	CLOUD FOR CUI **FedRAMP Moderate**
INCIDENT REPORTING **72 hours**	SUBCONTRACTORS **Flow-down, all tiers**	VERIFICATION **Self-attestation**

06 Have your say — two open comment windows

Both the CMMC pause and the FAR CUI rule are still taking shape, and the government is actively asking for industry input. This is a rare chance to influence the requirements you'll live under — we can help you draft and submit on either.

CMMC **The DoW RFI**

As part of the pause, DoW issued a **Request for Information** seeking DIB feedback on CMMC. The 60-day Reform Task Force will synthesize the responses — making this a genuine opportunity to shape where the program lands.

FAR CUI **FAR Case 2026-001**

Public comments on the proposed FAR CUI rule are open on the Federal Register — a compressed 30-day window to weigh in before it finalizes for all civilian contracts.

▶ COMMENTS DUE JULY 23, 2026

What to do next

Your path depends on one thing: whether you're already working with us. Either way, here's exactly where you stand.

CURRENT CSS CLIENTS

You're covered — there's nothing you need to do.

If you're already a CSS client, relax. Your program is in motion and **you are on track**. We will continue our onboarding efforts and ongoing operations exactly as planned — maintaining your self-assessment, keeping your SPRS score and SSP current, and driving any open POA&M items to closeout — so that you are **ready the moment the certification requirement returns**. No action is required on your part. You will hear from us as the 60-day review resolves and the certification path becomes clear — before it affects you. If you have questions in the meantime, your onboarding coordinator is your direct line (see below).

NOT YET A CLIENT

Use this window to get to a defensible posture — with us.

The pause is the ideal time to close the gap — before the deadline returns and demand for assessors spikes and prices climb. Here's the path we'd put you on, and where our fixed-scope, one-time services make it fast and predictable:

1. **Complete your self-assessment.** Get an honest score against all 110 NIST 800-171 controls — validated, not guessed. ◆ ONE-TIME: CSS Self-Assessment Validation
2. **Report your score to SPRS.** Post a current, accurate self-assessment score and senior-official affirmation.
3. **Correct your POA&M items within 180 days.** Remediate open items and complete the closeout self-assessment on the clock.
4. **Update and finalize your SSP.** Make sure your System Security Plan matches your real environment and stands up to scrutiny. ◆ ONE-TIME: CSS SSP Finalization

When it comes to doing this right, on time, and audit-ready — **Cyber Security Solutions is the partner to choose.**

YOUR POINTS OF CONTACT

NEW & PROSPECTIVE · GENERAL INQUIRIES

Justin Martin

DIB Developer

jmartin@securedbycss.com

Contact for: becoming a client, service questions, and any inquiry not tied to an active engagement.

CURRENT CLIENTS

Roberto Torres

Lead Onboarding Coordinator

rtorres@securedbycss.com

Contact for: all questions related to your active onboarding and ongoing compliance operations.